Threat Hunting Made Easy!


# TXHunter – Endpoint Threat Hunting

## THREAT HUNTING

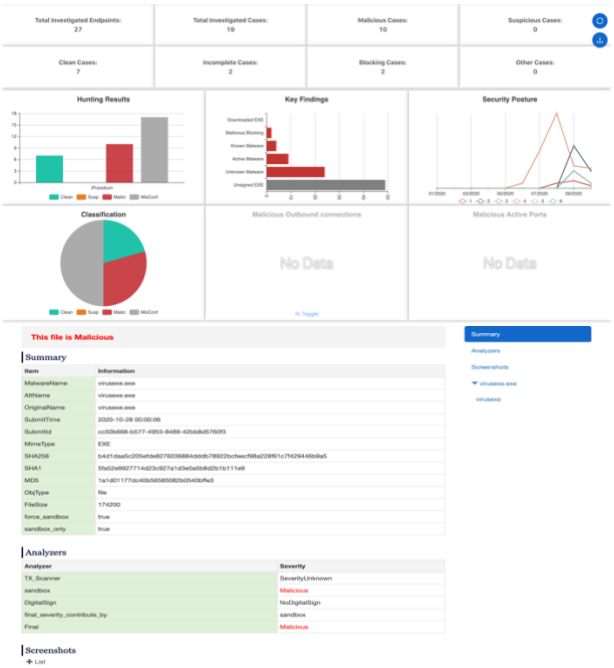
TXHunter integrates with SIEM & SOC workflow systems via RestAPI to selected endpoint systems to investigate and pass behavioral data back.

## IT SUPPORT

TXHunter enables IT support teams to remotely investigate unstable systems to identify if they have been compromised by malware before requiring re-imaging or system updates.

## SECURITY OPERATIONS

TXHunter enables security teams to verify in minutes, if a high value laptop has been compromised while off the corporate network.




TXHunter is a new generation of machine-assisted hunters used for conducting highly focused threat incident investigations remotely. You only need to tell TXHunter which endpoints you want to investigate, download the disposable run-time agent to gather the data and wait for the analysis.

The agent takes a snapshot of the suspicious system and automatically conducts an incident investigation. If the investigation process identifies suspicious files or URL links, it will automatically launch the built-in sandbox capabilities for a behavior analysis. TXHunter can also integrate with third party engines and intelligence platforms, to provide additional context on detected objects.

- Performs endpoint, desktop or server breach investigations remotely with no permanent agent required. A continuous monitoring option available for systems that need to be baselined.
- The real-time threat hunting tool gathers the attack evidence, including memory, log and suspicious objects (PE, document files and URL's) in order to do automatic incident analysis.
- Detects APT's, backdoors, spyware, hidden processes and rootkits, unusual network connections, mis-configurations and past abnormal activities.

## ADJUDICATION

In approximately 5 to 10 minutes, TXHunter provides a straight and clear answer whether an endpoint has been infected or hacked, the severity level of that action and all supporting data needed to remediate the incident.


**Final Result:** Malicious
**System Critical Level(SCL):** Very High ★ ★ ★ ★ ★
**Conclusion:** Detected Evidence of the following: [Detected suspicious file.] [Detected suspicious process.]

**Endpoint ID:** 1542d637-e927-430a-8e14-40280a7ff363
**Case ID:** ac48d677-4c45-406d-b2ba-789e487cfad3
**User Name:**
**OS Name:** Microsoft Windows 10 Pro
**OS Version:** 10.0.18363 N/A Build 18363
**Host Name:** DESKTOP-27HBHV9
**IP4 Address:** 192.168.194.186
**MAC Address:** 00 0c 29 38 ef d5
**Investigator:** AdrianaBabino
**Organization:** iPresidium
**Agent Version:** 3.1.7.210
**Hunting Time:** 10/29/20 16:35:34 Eastern Daylight Time
**Hunting Mode:** TXShield
**Baseline:** yes

iPRESIDIUM


# Service Features and Benefits

### SANDBOX TECHNOLOGY

Analyzes unknown file and URL links according to their behaviors to detect new malware. 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.

### TXShield

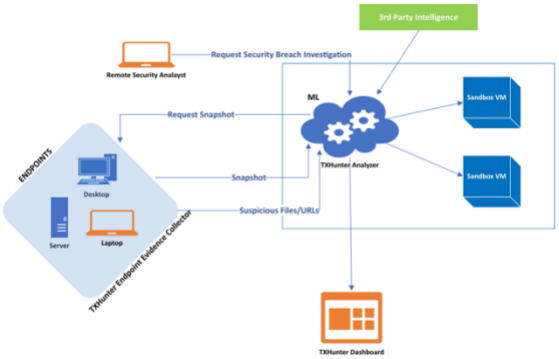
Protects endpoint and data center systems against zero-day attacks without requiring patches.

### iPRESIDIUM

Is a cybersecurity and risk advisory firm. We provide end-to-end enterprise security solutions and services for private and public entities of all sizes. iPRESIDIUM helps customers protect their business, employees, data and their reputations.

For more information on TXHunter or any of our solutions or services please visit us on the web at:

**www.ipresidium.com**




Information Security teams who are investigating potential breaches are often required to deploy endpoint detection response (EDR) sensors across the network environment to try and pick up evidence of system breaches or data exposure. This is the equivalent of casting a wide net to try and collect as many fish as possible, but not knowing exactly where they are, or what they are.

In contrast , by leveraging the TXHunter solution, incident response (IR) teams are able to quickly deploy a disposable client to suspect systems to promptly identify the presence of unknown and suspicious files on critical production Windows servers or endpoint systems. This allows the IR team to determine the extent and severity of the incident for risk analysis and remediation as early in the investigation process as possible.

# System Requirements

- **Endpoint Systems:**

  Windows 7 SP1, Windows 8.1, Windows 10, Windows Server 2008 R2, 2012, 2012 R2, 2016, 2018
  Linux: CentOS 6.0+, Ubuntu 12.0+ and Redhat 6.0+
  Mac OS 10.15+

- **Analyzer Server:**

  Deployable on Physical Server, VMWare/ESXi, VirtualBox, Cloud (ISO Image CentOS 7.2)

- **Snapshot Data:**

  ~3 MB in size – Data sent in secured container transmitted via Windows Sockets API

- **3rd Party Intelligence:**

  Can run in isolated mode for sensitive networks, or configured to use intelligence feeds via REST API (VT)

- **Report Format:**

  HTML, PDF and JSON

### DATA COLLECTED

- System Information
- Process Information
- Network Information
- Autorun Information
- Event Information
- Policy Information
- File Information
- Driver Information
- Kernel Information

620 Newport Center Drive, Suite 1100 | Newport Beach, CA 92660 | Phone: 949.721.6612 | Fax 866.205.2904 | Info@ipresidium.com