FireTower
Mobile Incident Response Kit

Standard Practice for IR

FireTower IR Kit uses standard industry practice for forensic analysis by focusing on persistence to find the compromise

Integration and Automation

FireTower IR Tools comprise unique integrated and automated forensic tools for Zero-day attack incident investigation

Portability

FireTower IR Kit can be preloaded on USB flash drive and ready for investigation once on-site and is a must-have emergency tool in IR jump bag

Accessibility

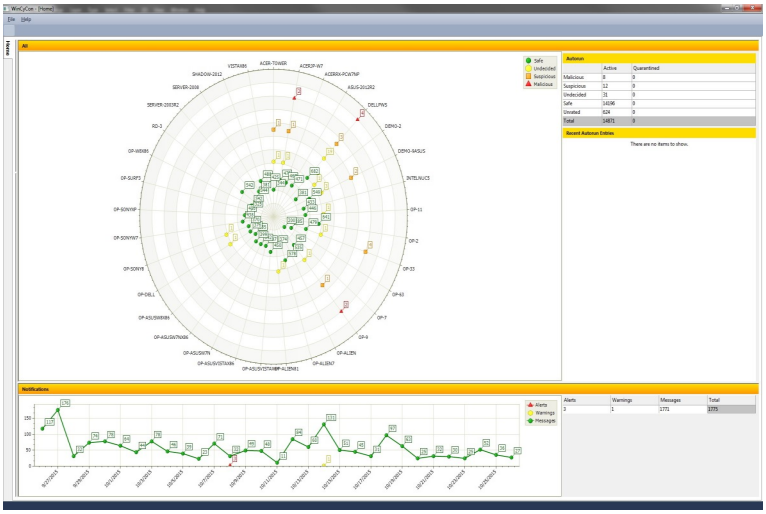
FireTower Triage Workbench can be accessed locally or remotely using Windows console

Supported Endpoint OS

Windows XP/Vista/7/8/10
Windows Server 2003, 2008, 2012

Supported FireTower Service OS

Windows 7/8/10 &
Windows Server 2008, 2012



FireTower Mobile IR Kit Features:

- Portability
  - Preloaded on USB
  - Ready to Run
- Security
  - Self-Contained
  - No cloud resources needed
- Continuous Monitoring
  - Discover Zero-day Malware
- Network Operation
  - Commands to all at-risk PCs
- Optional Investigation Tools
  - Automation/Integration
  - Volume Shadow Copy Based
  - Life Cycle Change Detection
- Minimum Training
  - just Windows Supports

FireTower mobile incident response kit is designed as an emergency tool to facilitate the collection of the critical Indicators of Compromise (IOCs) at the moment an incident investigation is initiated. This FireTower Mobile IR Kit enables incident response investigators to confirm a breach, identify suspicious or malicious IOCs and their timeline, and initiate containment and remediation processes without unnecessary delay.

FireTower Mobile IR Kit is an integrated and automated collection and analysis tool set for these critical IOCs following the standard practice used by most incident response investigation. It is a must-have investigation tool in the incident response jump bag whether you are a specialized first response team or a scratch team assembled to deal with an immediate security incident.

The FireTower Mobile IR Kit compromise a customized Windows FireTower Security Solution with optional postmortem forensic tools: AutorunCheck and ConfigSafe. AutorunCheck Forensic Edition is a system diagnostic software designed to expedite the process of identifying and verifying the persistence mechanisms in Microsoft Windows PCs including Volume Shadow Copies of system states. ConfigSafe is Windows configuration management software designed to expedite the process of identifying system configuration changes through Volume Shadow Copy Services.

FireTower Mobile Incident Response Kit can be preloaded on a Windows laptop, Intel NUC, or even USB flash drive and carry to customer's site by first responder team and is ready to perform evident collection and forensic analysis, and can be removed easily for off-site forensic analysis and incident report.

All the collected incident response data are self-contained on the FireTower Service database which is resided on that laptop, NUC, or USB flash drive for security purpose.

SAMPAN security inc

info@SampanSecurity.com
www.SampanSecurity.com

Malware is already inside your network!

Breaches are pervasive and businesses of all sizes have to deal with cyber security threats to avoid damage to their business operation, reputation, liability, and customer privacy. Large corporations throw money and resources into the fight and still fail to prevent breaches, but small and medium-sized enterprises (SMEs) with much smaller budgets are also fast becoming targets of opportunities. Stopping a targeted attack without properly trained incident responders and resources is an overwhelming task.

Since it is impossible to provide complete prevention at the endpoint perimeter, the question is not "If you will be breached?", but "When?". Enterprises need a cost-effective incident response plan ready to launch every time a cyber intrusion or attack is discovered. Once an incident response is initiated, the main goal is to quickly collect forensic data from hundreds or thousands of endpoint computers for triage analysis and identify at-risk systems for further incident investigation. According to one industry report, for a small business of 100 endpoint computers, a single incident response could cost over $15,000. The cost of FireTower Continuous Monitoring service with instantly available forensic data can pay for itself after just a single incident.

Why Persistence Mechanisms?

Persistence mechanisms are used in modern operating systems to allow applications to start automatically after system reboots or according to a specified schedule. Microsoft Windows operating systems, for example, use "Autoruns" to accomplish this. Malware and Zero-day attacks alike commonly abuse persistence mechanisms built into operating systems in order to gain a foothold and dwell on a PC after it has successfully infiltrated the PC's perimeter defense.

As Zero-days are previously undiscovered and have no associated signature, traditional detection methods and perimeter-based defenses fall short of stopping them. An unconventional strategy is required to protect against Zero-days. FireTower Guard identifies unknown, potentially malicious Zero-day software by analyzing persistence mechanism change events in real-time. By starting at the endpoint and monitoring for persistence mechanism change events initiated by software, which could be legitimate or malicious, Zero-day attacks can be identified and tagged as potentially dangerous software.

This approach is validated by the fact that focusing on persistence mechanisms is already the industry standard practice for incident response and forensic investigation. Most forensic investigations initiate the incident response process by examining persistence mechanisms as it is a fast and effective method for assessing malware incidents and discovering breaches and malware. Most, if not all, recently reported cyber security Zero-day attack incidents involved persistence mechanisms.

A single Microsoft Windows PC contains hundreds of Autorun settings which makes identifying and verifying their validity a time-consuming process. In a corporate, intelligence, or military environment with hundreds or thousands of PCs, this process becomes impractical to accomplish through manual software tools. Automated tools are crucial for allowing support professionals and digital forensics investigators to perform their jobs more effectively and efficiently.

Inter-Host Intrusion Prevention System (IHIPS)

Gartner's report suggests that an effective security solutions should include continuous monitoring for patterns and behaviors indicative of malicious intent. Within an enterprise environment, continuous monitoring must be implemented with a measured approach. A key factor in a measured approach for continuous monitoring across the enterprise is the persistence mechanism change events. The detection of an unauthorized or malicious persistence mechanism change event could signal an intrusion to the target endpoint computer. The detection of multiple instances of unauthorized persistence mechanism change events across different hosts could signal targeted attacks in progress and lateral movement of malware within the enterprise network.

Inter-Host Intrusion Prevention System (IHIPS) continuously monitors enterprise critical forensics at endpoint computers and stacks the data in the enterprise threat database. FireTower Console with IHIPS technology is capable of detecting attacks in progress in the enterprise and identifying lateral movement of targeted or multi-stage attacks in progress.