FireTower Guard™

Zero-day Attack [Detection, Containment, Forensics

Close the gap in cybersecurity

Zero-day attacks — in spite of today's layers of protection — bypass installed antivirus solutions and remain the most elusive malware. In most cases, zero-day attacks depend upon modifying the Autorun service in the Windows operating system to survive the reboot process and to maintain control of the target PC. Autorun settings have long been used by system administrators and digital forensic investigators to resolve everything from crashes to cyberattacks. However, the tools available for such analysis can only be used after-the-fact and the data garnered requires expert subject matter knowledge and long effort. FireTower Guard solves these problems through the introduction of *Autorun Tagging* and *Cloud-based Authentication*. The result is both a software utility that detects and contains zero-day attacks and a software tool that simplifies forensic analysis, closing a critical gap in cybersecurity.

FireTower Guard complements and works side-by-side with traditional antivirus and other cybersecurity solutions.

Detection

FireTower Guard's Autorun Tagging monitors Autorun creation and changes in real-time. Upon discovery of Autorun changes, it accesses Cloud-based systems to identify and authenticate via both MD5 and SHA-1 hash functions.

Automated authentication is made possible in part through the Autorun Setting Repository (ASR), hosted by Sampan Security. The repository is backed by a hot standby ASR and is complemented by versions localized for specific countries/regions. An enterprise Intranet ASR Proxy is available for SCIF sites and other sensitive network environments.

- **Green**: Certified entry in Autorun Setting Repository
- **Yellow**: Zero-day Autorun setting (benign or malicious)
- **Red**: Known malicious Autorun setting

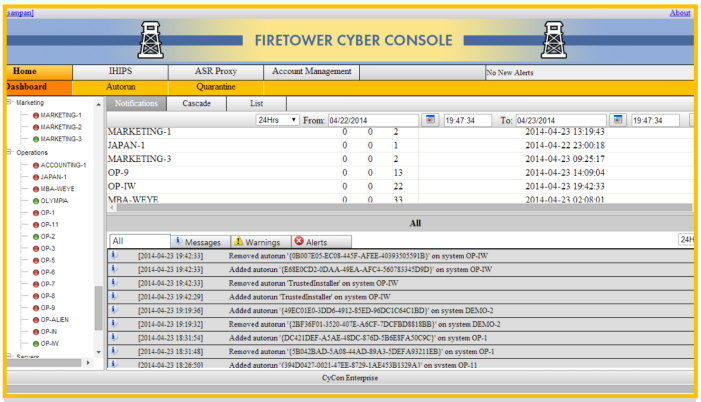
Containment

The software can automatically contain risky Autorun settings such as known-malware entries, suspicious behavior such as putting a binary in the alternate data stream, or auto-reinsertion of a non-certified Autorun setting. Autoruns are assigned ratings that advise the user and initiate protection:

- **Off**: Monitoring-only mode
- **Normal**: Block known malicious or suspicious settings
- **Elevated**: Block all except authenticated setting changes
- **Lockdown**: Block all except authenticated system changes

Forensics

Unlike traditional digital forensic investigations, FireTower Guard automates the analysis of Autorun setting changes.



Centralized consoles simplify protection, management and analysis

For example, consider the effort to investigate a cyberattack upon a typical office network of 3,000 endpoints. At an average of 400 Autorun settings per system, investigators would face about 1.2 million settings. In contrast, if FireTower Guard were to be utilized — even after-the-fact — it would authenticate *all Autorun settings automatically.* As a result, the frequency analysis that investigators would focus on would likely drop from 3,000 to perhaps 5 compromised systems and all malicious or suspicious settings would be immediately presented.

Zero-day Protection and Investigation for:

- Forensic Investigator
- Security Consultant
- IT Administrator
- Training Facilitator
- Solution Provider
- ISV & IHV Companies

Components

FireTower Guard has several key components: a PC-based endpoint threat detection module, an Autorun Settings Repository (ASR), and a server-based intrusion prevention system with a web-based cybersecurity management console (CyCon). The endpoint module monitors Autorun changes in real-time and automatically checks with the ASR. The ASR authenticates the changes, enabling containment when malware is identified. In an enterprise configuration, the end-point data is incorporated in an Inter-Host Intrusion Prevention System (IHIPS) that maintains the threat database, ASR proxy and threat analytic algorithms. The Web-based console, CyCon, allows all systems to be monitored and managed regardless if the systems or the investigators are onsite or remote and whether they are company IT staff or consulting forensic investigators.

SAMPAN security inc
74 Northeastern Blvd.
Nashua, NH 03062 USA
info@SampanSecurity.com
www.SampanSecurity.com