Testoodo SRL

We play with cybersec.

Our job

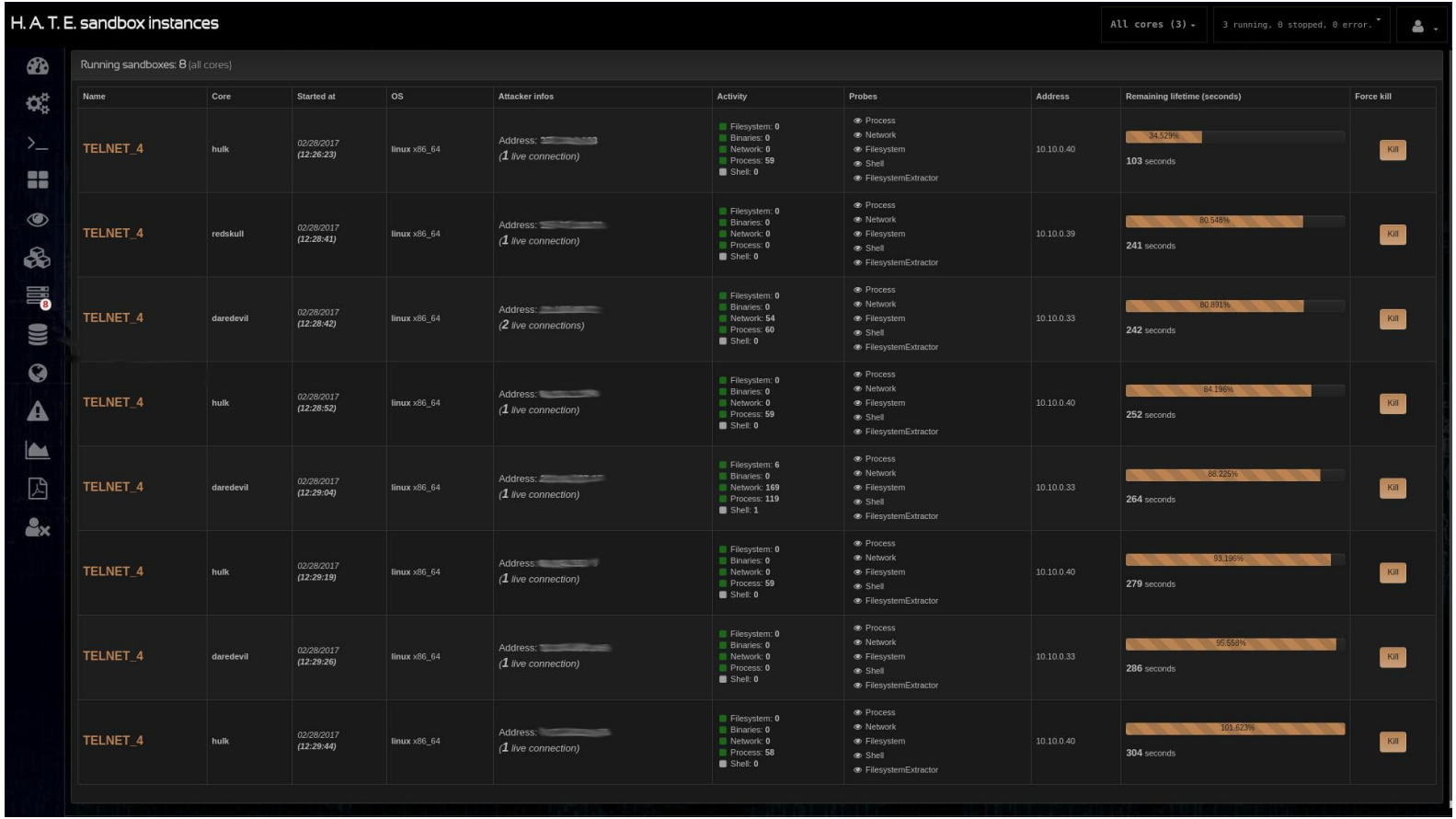
- Malware analysis
- High Interaction Passive Defensive Systems - Honeypot
- Cybersec R&D
- Penetration Testing
- Cyberspace surveillance

Our product: H.A.T.E.

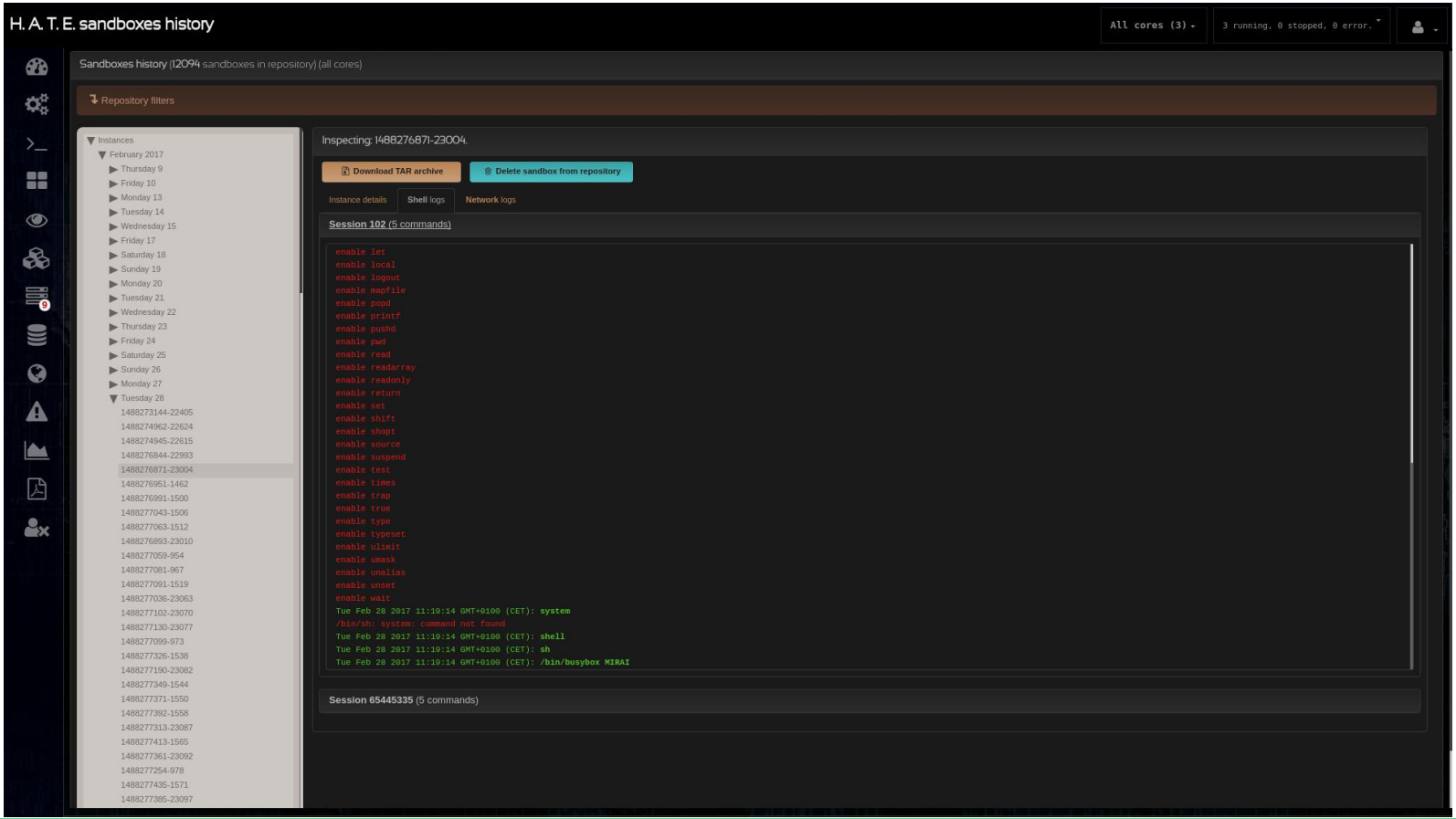
Honeypot-based Analysis Threat Engine

- Is a distributed system. Each instance is a core. Cores are coordinated by a control center.
- Each core schedules honeypot based on real operating systems. Once the attacker instantiates a connection he gains its own sandbox (of course for a limited amount of time). Subsequent connections from the same IP are redirected to the same sandbox.
- Network, File System, Process Execution and Console operations are tracked and stored.
- Each one of the previous is a specialized probe which can be injected into the system on demand. Probes can be written in any programming language.

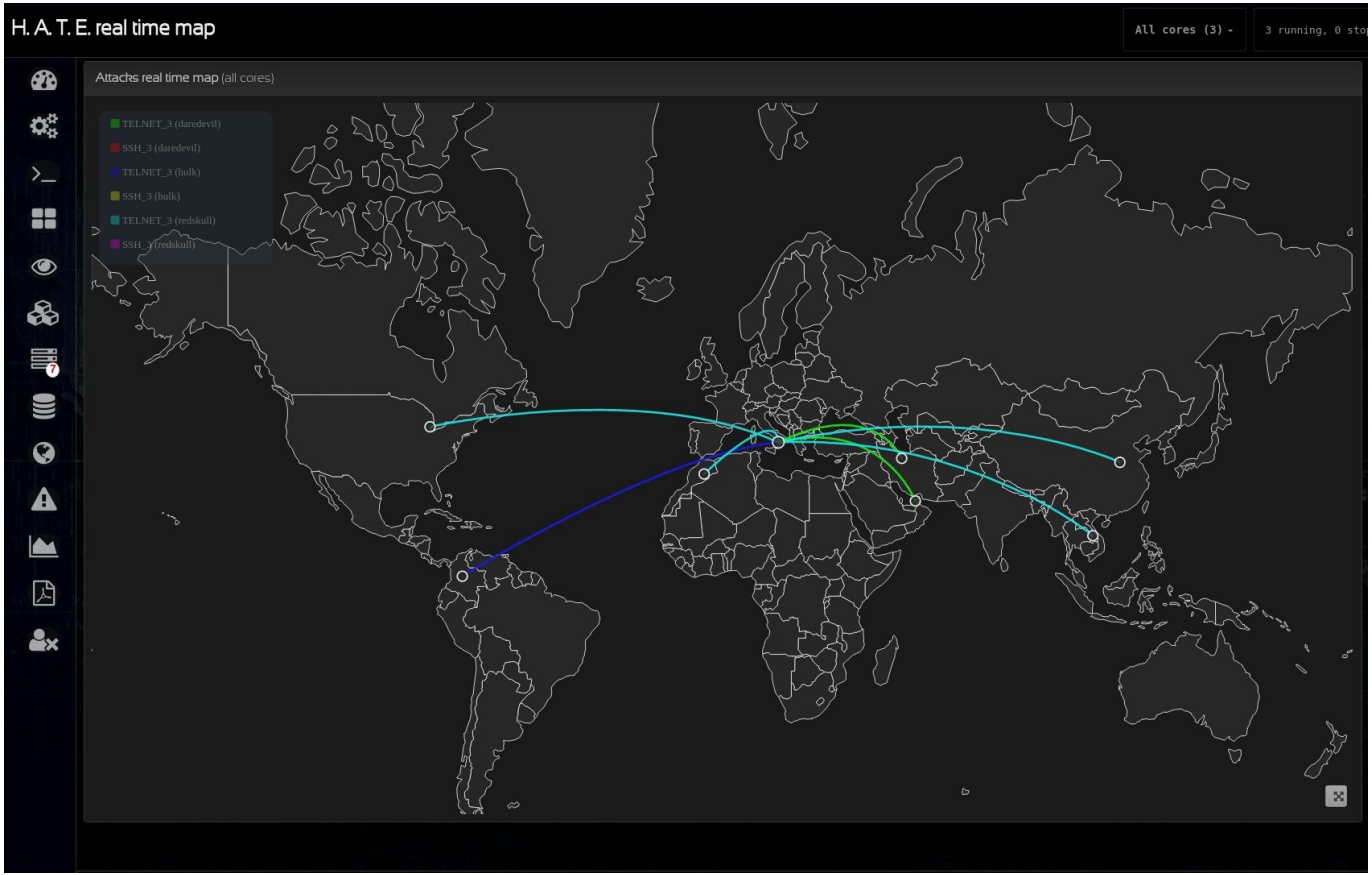
Realtime sandbox monitoring



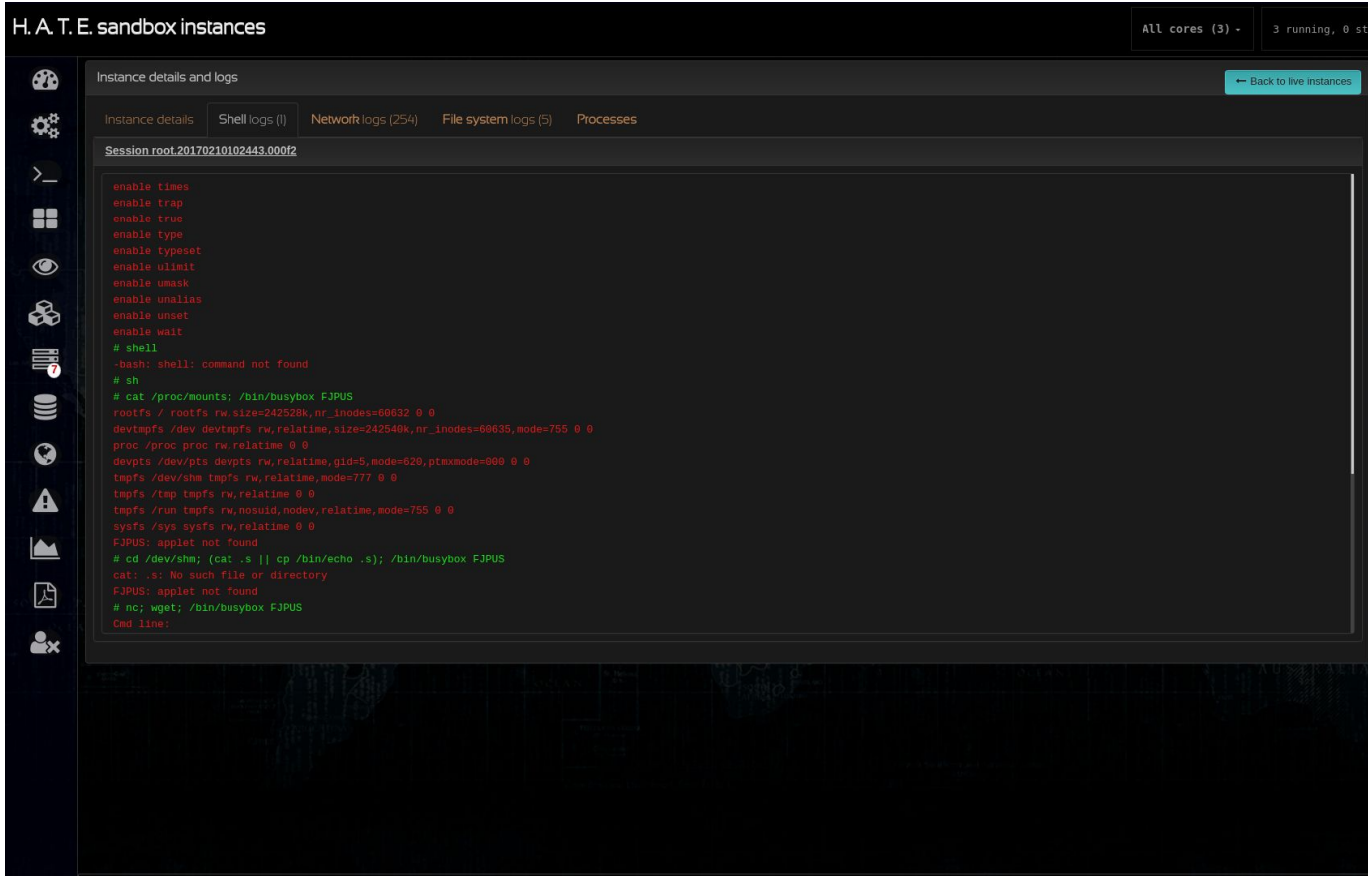
Attacks storing and retrieving



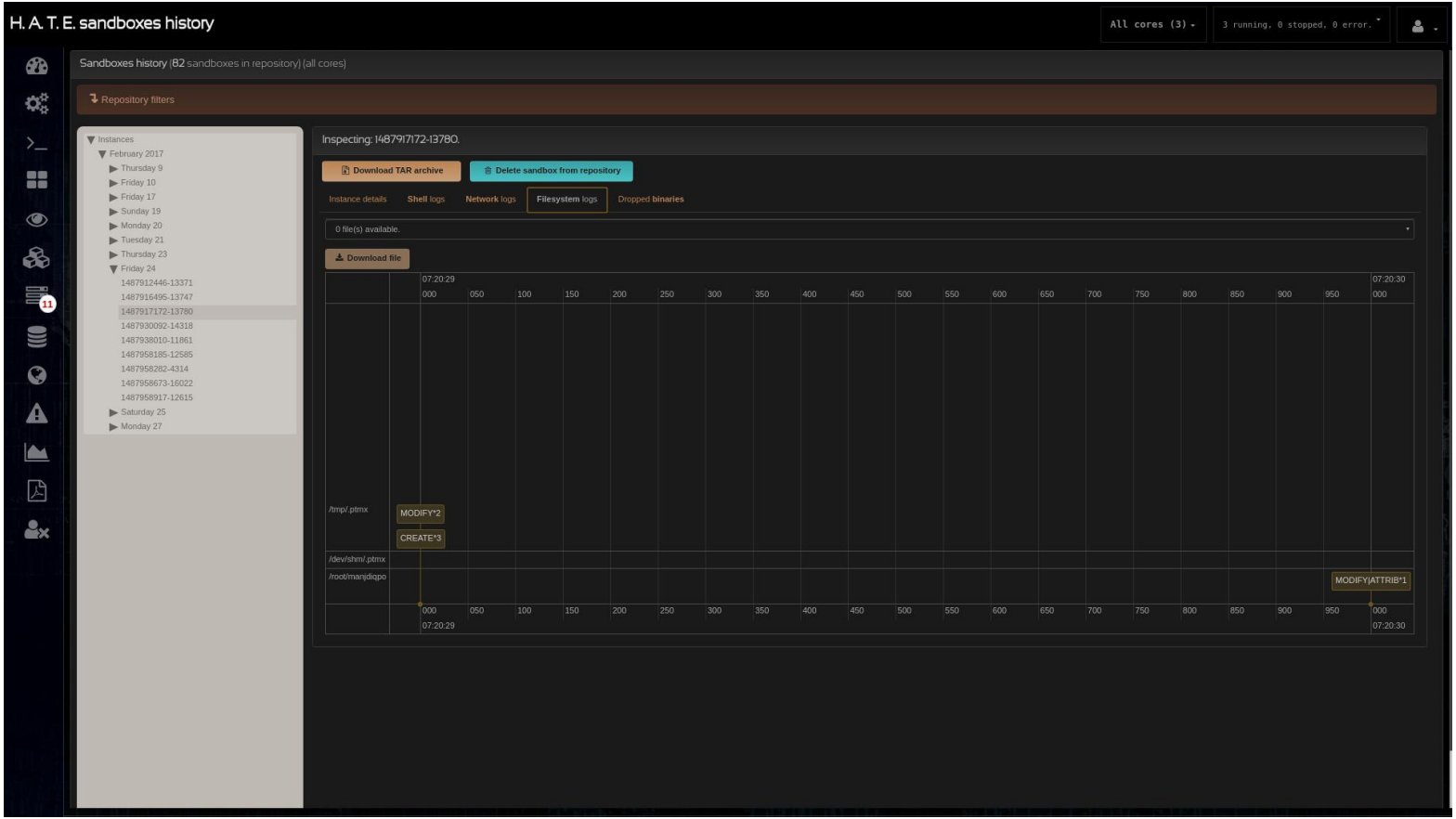
Realtime worldwide map of attacks



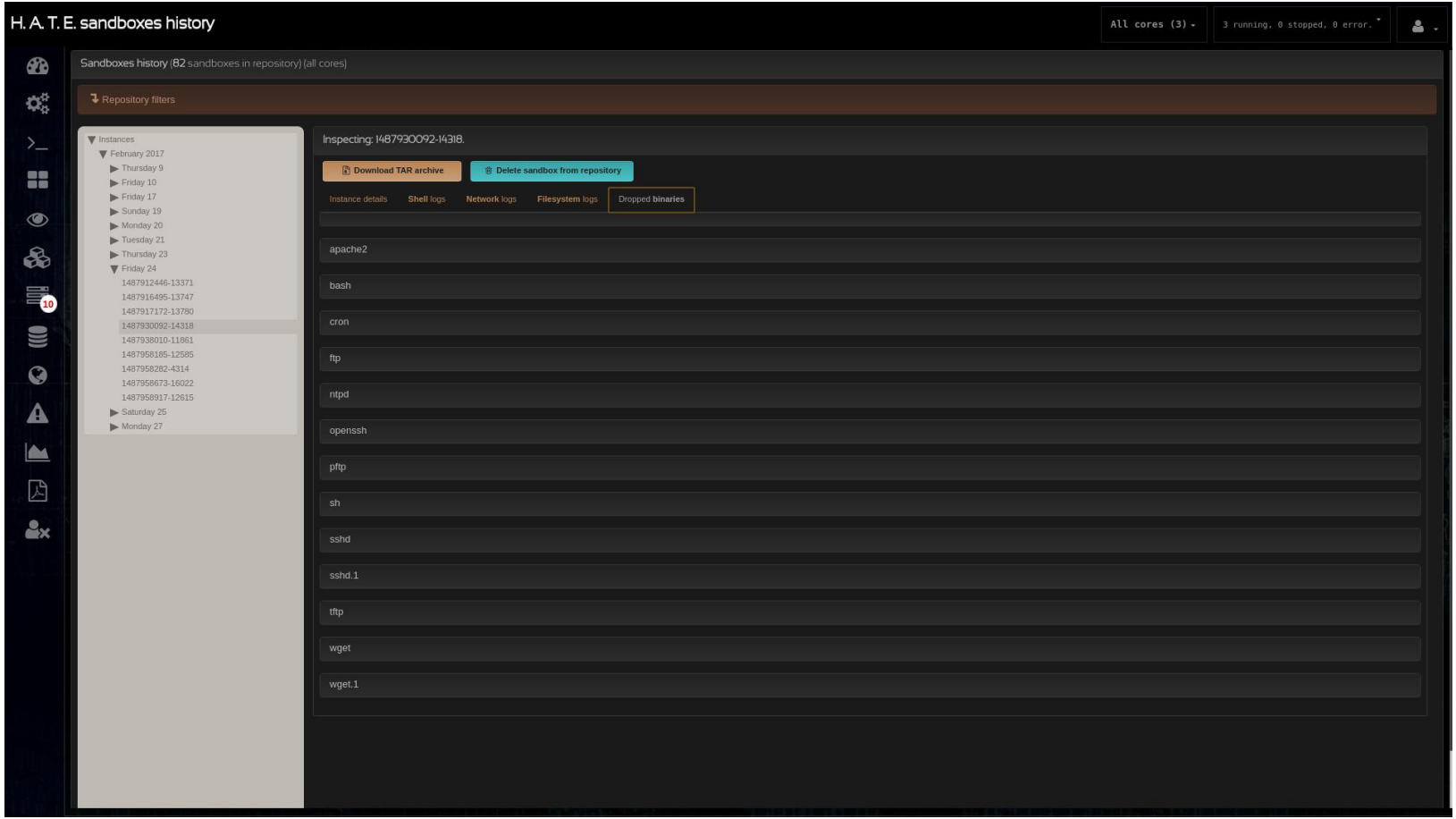
*Nix Console Monitoring and logging



Filesystem actions tracking



Download and view the downloaded malware



Lot of other features.
If you are curious contact us.