Threatray @ CERN

Roman Shumaylov

09.06.2023

Motivation

We can never be 100% secure, but at Security Team we use every opportunity to increase this % at least a little bit.

Threatray

- Swiss cybersecurity company
- Code reuse analysis for malware detection
- Binaries/files analysis
- Memory dumps analysis
- Capable of identifying ~1500 malware families

Our use case

- Scheduled task on Windows machines to run memory scan once a week

- Threatray binary:

1. Scans memory of running processes
2. Identifies suspicious memory regions
3. Packs them into an archive (no personal information uploaded)
4. Uploads scan to Threatray backend
5. In the backend analyzes code of memory segments for malware detection

DEMO

How much?

- **Mutually beneficial agreement between CERN and Threatray**
- **They get to test and feedback – We get their product for free!**

Current status

- **Deployed at IT-CD group at test stage**
- **Goal – deploy for all CERN hardened Windows PCs (~500 machines)**

home.cern