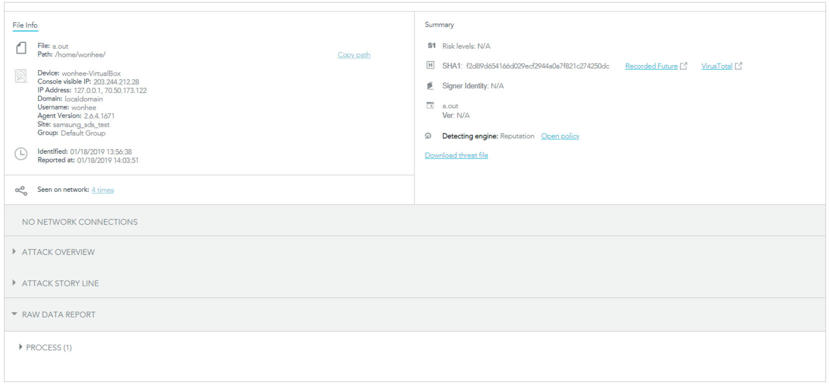
SentinelOne Use Case

Easy-to-use attack analytics powered by AI (Workflow search)

Easily analyze attacks with Sentinelone engine's visualization of malware analysis, overview and story line.

Analyze



File Info

File: a.out
Path: /home/wonhee/

Copy path

Device: wonhee-VirtualBox
Console visible IP: 203.244.212.28
IP Address: 127.0.0.1, 70.50.173.122
Domain: localdomain
Username: wonhee
Agent Version: 2.6.4.1671
Site: samsung_sds_test
Group: Default Group

Identified: 01/18/2019 13:56:38
Reported at: 01/18/2019 14:03:51

Seen on network: 4 times

Summary

S1 Risk levels: N/A

SHA1: f2d89d654166d029ecf2944a0a7f821c274250dc Recorded Future VirusTotal

Signer Identity: N/A

a.out
Ver: N/A

Detecting engine: Reputation Open policy

Download threat file

NO NETWORK CONNECTIONS

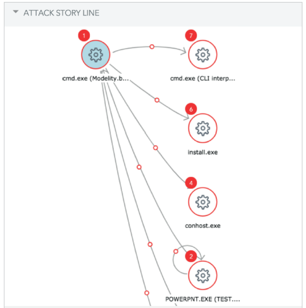
ATTACK OVERVIEW

ATTACK STORY LINE

RAW DATA REPORT

PROCESS (1)

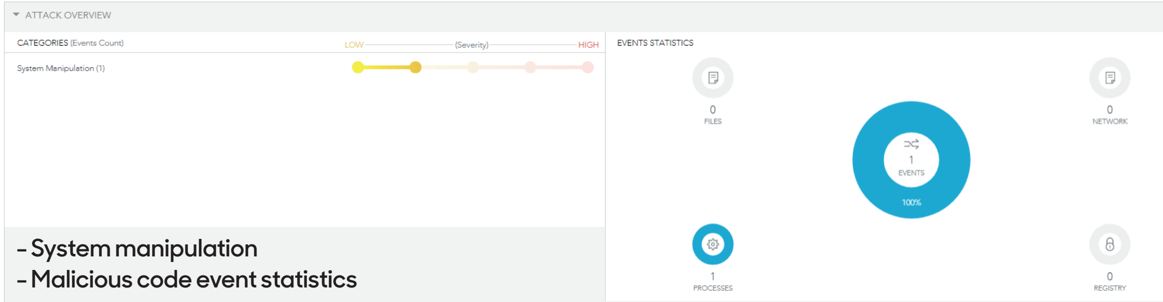
Attack Story Line



ATTACK STORY LINE

- Malicious code story line
- Activity log

Attack Overview



ATTACK OVERVIEW

CATEGORIES (Events Count)

System Manipulation (1)

EVENTS STATISTICS

- System manipulation
- Malicious code event statistics

SAMSUNG SDS