CIRCL
Computer Incident
Response Center
Luxembourg

Latest Kunai Updates

An Open-Source Threat-Detection Tool for Linux

https://github.com/kunai-project/

Quentin JEROME

2024/10/22

Hack.lu - Luxembourg

The idea in short

Having an **open-source** and **free** Sysmon[1] (Microsoft) equivalent for **Linux**

But why?

- Help **incident responders**
- Threat hunting and detection

Enable you to improve your visibility on you Linux endpoints

[1] https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Main features

- **Monitor** and **log** many **events**[2] (execve, shared object loaded, BPF programs loaded, files read/write/delete . . .)
- Events comes with the following:
  - Relevant information to build solid **behavioral detections**
  - In chronological order
  - Group **process/task** activity through a uuid
  - **Task ancestors** tracking
  - Enriched with data from previous events (i.e. network connect/send)
- Accurately track security events generated by **Linux container** solutions

[2] https://why.kunai.rocks/docs/category/kunai—events

Detect and React

```
# name of the rule
name: mimic.kthread
# acts as a pre-filter to speed up engine
match-on:
    events:
        # we match on kunai execve and execve_script event ids
        kunai: [1, 2]
matches:
    # 0x200000 is the flag for KTHREAD
    $task_is_kthread: .info.task.flags &= '0x200000'
    # common kthread names
    $kthread_names: .info.task.name ~= '^(kworker)'
# if task is NOT a KTHREAD but we have a name that looks like one
condition: not $task_is_kthread and $kthread_names
# severity is bounded to 10 so it is the maximum score
severity: 10
```

Any rule may encode **actions** to take on a given detection

- **kill**: kill the process triggering the detection
- **scan-files**: scan files with **Yara** rules

Same format **modulo a boolean** parameter can be use to craft powerful **log filtering rules**

Many other stuffs

- Configurable with **IoCs**
  - straightforward format
  - integrated with/in **MISP**[3]
- Scan files with **Yara**
- Correlate with network logs thanks to **Community ID**[4]
- Run samples in **sandbox**[5] and monitor it with Kunai help building detection rules
- Install it as a **systemd** unit
- Can be run in **harden** mode to self-protect
- Supported architectures: **x86-64**, **aarch64**

[3] https://github.com/MISP/MISP/releases/tag/v2.4.199
[4] https://github.com/corelight/community-id-spec
[5] https://github.com/kunai-project/sandbox

5min pass fast!

If you like the project **star it**, **use it**, **give feedbacks**

GitHub: https://github.com/kunai-project/

X/Twitter: @kunai_project

Mastodon: @kunai_project@infosec.exchange

LinkedIn: https://www.linkedin.com/company/kunai-project/