



Suricata Landlock Support

How in-person conference can improve software.

About Me

Stamus Networks

- Co Founder
- CTO

Social Media

- @regiteric on Twitter (#jesors)
- <https://www.linkedin.com/in/ericleblond/>



Mickaël Salaün at Pass the Salt Conference

- Sandboxing your application with Landlock, illustration with the p7zip case
 - By Mickaël Salaün
 - Author of Landlock
 - Linux kernel developer at Microsoft
- Video:
<https://passthesalt.ubicast.tv/videos/sandboxing-your-application-with-landlock-illustration-with-the-p7zip-case/>
- A practical introduction on adding landlock support to software
- Info on the project: <https://landlock.io/>
 - Added in Linux 5.13
 - After 3 years of fight

Linux Kernel Developer at Microsoft

- We come from far
- One of my first open source t-shirt (from 2004)



Landlock concept

- Restrict ambient rights (e.g. global filesystem access)
- Per process
- Declaration of access rights done by process
 - Process start
 - Declare what access it needs
 - In which directories it will write
 - In which directories it will read
 - ... more access settings
 - Enforce the policy
 - Run active code
 - On unsecure data

Landlock in one image



If I fits I sits **ACTIONS**

imgflip.com

Risk assessment of Suricata

- Suricata in sniffing mode
 - Read configuration file
 - Overwrite files (running as privileged user)
- Suricata in pcap reading mode
 - File modifications as user
 - Parsing untrusted data
 - Pcap with potential active attacks

Configuration

<https://suricata.readthedocs.io/en/latest/configuration/landlock.html>

```
1108
1109 security:
1110     # if true, prevents process creation from Suricata by calling
1111     # setrlimit(RLIMIT_NPROC, 0)
1112     limit-noproc: true
1113     # Use landlock security module under Linux
1114     landlock:
1115         enabled: yes
1116         directories:
1117             #write:
1118             # - /home/regit/builds/suricata/var/run/
1119             # /usr and /etc folders are added to read list to allow
1120             # file magic to be used.
1121             read:
1122                 - /usr/
1123                 - /etc/
1124                 - /etc/suricata/
1125
```


Suricata case

- Easy determined interactions with file systems:
 - Read signatures & configuration
 - Write log files
- Specific values can be analysed from:
 - Configuration files
 - Command line option

Demo

- From command line
- Custom build

```
9/11/2022 14:59:33 - <Perf> - using shared mpm ctx' for ip.src
9/11/2022 -- 14:59:33 - <Perf> - using shared mpm ctx' for ip.dst
9/11/2022 -- 14:59:33 - <Perf> - using shared mpm ctx' for ipv4.hdr
9/11/2022 -- 14:59:33 - <Perf> - using shared mpm ctx' for ipv6.hdr
9/11/2022 -- 14:59:33 - <Config> - IP reputation disabled
9/11/2022 -- 14:59:33 - <Warning> - [ERRCODE: SC_ERR_FOPEN(44)] - could not open: "/home/regit/builds/suricata/etc/suricata/classification.config": Permission denied
9/11/2022 -- 14:59:33 - <Error> - [ERRCODE: SC_ERR_OPENING_FILE(40)] - please check the "classification-file" option in your suricata.yaml file
9/11/2022 -- 14:59:33 - <Error> - [ERRCODE: SC_ERR_FOPEN(44)] - Error opening file: "/home/regit/builds/suricata/etc/suricata/reference.config": Permission denied
9/11/2022 -- 14:59:33 - <Error> - [ERRCODE: SC_ERR_OPENING_FILE(40)] - please check the "reference-config-file" option in your suricata.yaml file
9/11/2022 -- 14:59:33 - <Config> - No rules loaded from /dev/null
9/11/2022 -- 14:59:33 - <Info> - No signatures supplied.
9/11/2022 -- 14:59:33 - <Config> - AutoFP mode using "Hash" flow load balancer
9/11/2022 -- 14:59:33 - <Config> - using 1 flow manager threads
9/11/2022 -- 14:59:33 - <Config> - using 1 flow recycler threads
9/11/2022 -- 14:59:33 - <Info> - Starting file run for /home/regit/Downloads/2019-07-05-Ursnif-with-Trickbot-and-IcedID.pcap
9/11/2022 -- 14:59:33 - <Notice> - Threads created → RX: 1 W: 12 FM: 1 FR: 1 Engine started.
9/11/2022 14:59:33 - <Info> - No packets with invalid checksum, assuming checksum offloading is NOT used.
```

Conclusion

- Available from Suricata 7.0
- Need at least Linux 5.13
- Easy to setup
- Feedback welcome

Questions ?

Thank You

Eric Leblond
CTO

el@Stamus-Networks.com