Threat Intel or threat ?

Éric Leblond

STAMUS NETWORKS

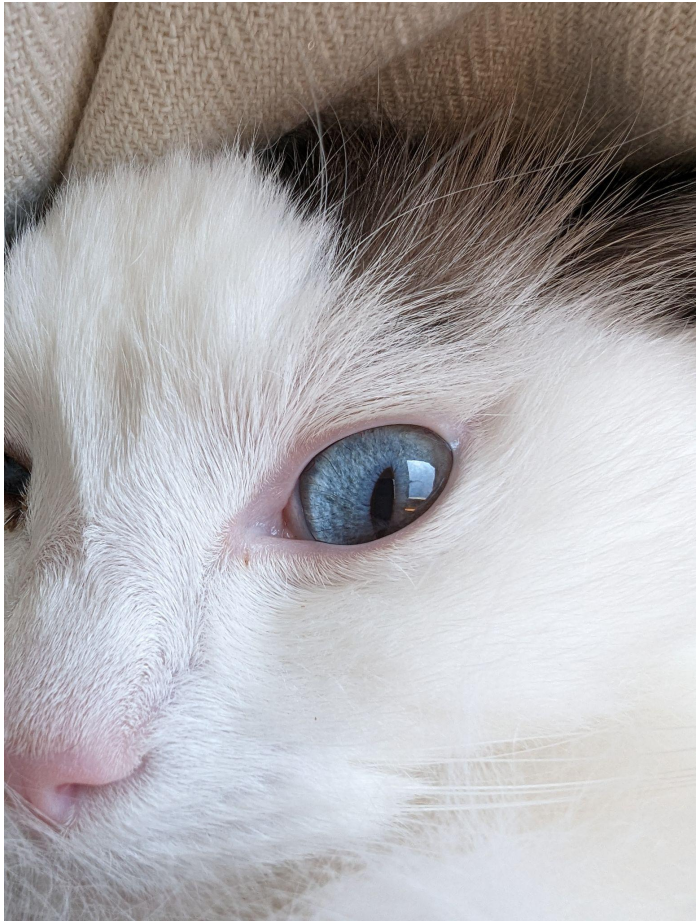
Who am I ?

Eric Leblond

- French
- Co founder & CTO of Stamus Networks
- Member of OISF’s board
- Contributor to Suricata since 2009
- Co-author of “The Security Analyst's Guide to Suricata”

Stamus Networks:

- Editor of a Suricata based NDR solution
- Contributor to Suricata



Evolution of signatures/threat intel distribution

- From a single source
  - Signatures from a single vendor
  - With potential local addition
- To multiple sources
  - Various source available of internet
  - OISF reference 12 public sources
- And extended threat intel exchanges
  - MISP
  - …
- Is there a risk of supply chain attack ?

Can threat intel be a threat ?

- Threat intelligence are input ingested in software
- The case of signature based systems
  - Various software
    - Suricata
    - Snort
    - Yara
  - Different features can be accessed
    - Some can exhaust resources
    - Some can be harmful ?

The case of Suricata

Lua support in Suricata (CVE-2023-35853)

- Run a lua script on demand

  Alert … (msg:”lua sig”; lua:sigscript.lua; …)

- Script is distributed with source of signatures as a separate file
- So arbitrary code can be run
- Problem:
  - If built-in, Lua is activated by default
- Fixes:
  - Disallow Lua in untrusted sources
  - Control Lua availability via config (suricata 6.0.13+)

Dataset (CVE-2023-35852)

- Handling of match on set of elements at high speed
- Option to enrich dataset from packet path
  - Tls.fingerprint; dataset:set,myset;
- Problem
  - Dataset:set,myset,type string, save /etc/password
- Fixes
  - Filter dataset usage in sources
  - No more absolute path (Suricata 6.0.13+)

Conclusion

- Suricata
  - Dataset is a design error
  - Lua is a feature that can be harmful
- Threat intel/Signatures are user input
  - Threat intel as signature needs to be controlled
  - Software using signatures need to be audited with that assumption in mind
- More information on Suricata vulnerability:
  - https://www.stamus-networks.com/blog/closing-a-suricata-supply-chain-attack-vulnerability
  - Suricata CVEs:
    - CVE-2023-35852 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35852
    - CVE-2023-35853 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3585