STAMUS NETWORKS

Suricata Language Server

Botconf 2023

About Me

Stamus Networks

- Co Founder
- CTO

Social Media

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

Open Source and Security

- Suricata
  - Developer
  - Board member of OISF
- Netfilter
  - “Emeritus” core team member

Writing Suricata Signatures

Bringing you own intelligence to threat intelligence

STAMUS NETWORKS

Writing Suricata Signatures

Some dare to say out loud what people are thinking quietly

Suricata Signature examples

Method Observed Malicious SSL Cert (Bazar Backdoor) / 1002032313

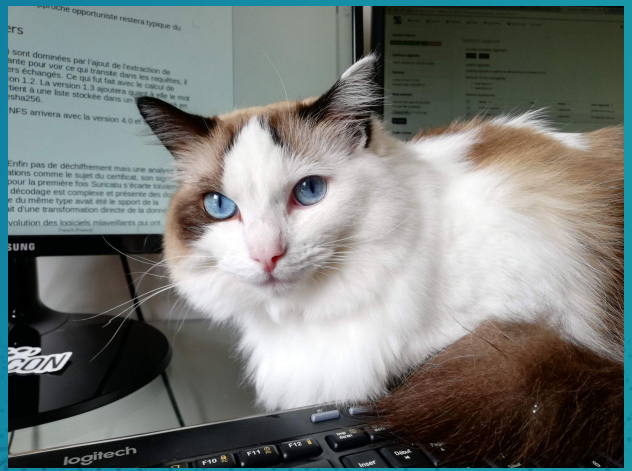
```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (Bazar Backdoor)"; flow:established,to_client; tls.cert_subject; content:"C=KZ, ST=Astana, L=Astana, O=NN Fern, OU=KZ System, CN=forenzik.kz"; bsize:66; fast_pattern; reference:url,twitter.com/z0ul_/status/1374121916143919106; reference:md5,4cf6fb8514073319e7759b4f66d13f08; classtype:domain-c2; sid:1002032313; gid:2; rev:1; metadata:attack_target Client_and_Server, created_at 2021_03_23, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2021_03_23, mitre_tactic_id TA0042, mitre_tactic_name Resource_Development, mitre_technique_id T1587, mitre_technique_name Develop_Capabilities;)
```

Process of signatures writing

- Writing Suricata Signatures can be a nightmare:
  - Syntax inherited from Snort
  - With important evolution
- It is a repetitive process:
  - Write a signature
  - Check syntax
  - Check it is matching
  - Refine the signature
  - Check performance
  - Refine the signature

Suricata Language Server

By a lazy one, for the lazy ones



STAMUS NETWORKS

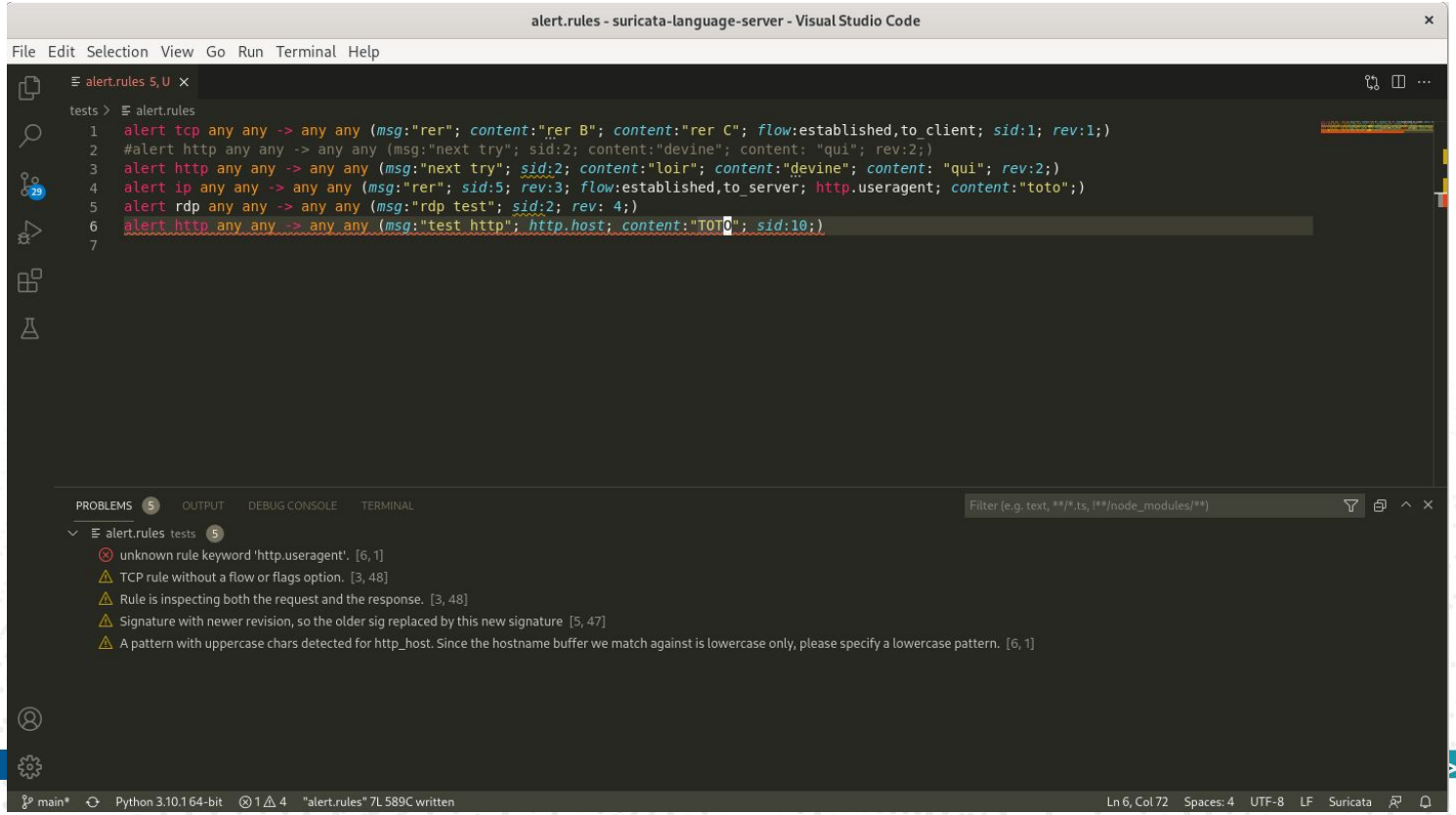
Excuse my French ? Language Server ?

- Language Server Protocol
  - Standardize communication between IDE/Text Editor and Language Server
  - Via JSON RPC
- Features
  - Auto complete
  - Go to definition
  - Find all references
  - Warnings
- More information:
  - https://microsoft.github.io/language-server-protocol/

Suricata Language Server

- A language server for Suricata signature
- Will get you
    - Syntax checking
    - Performance hints
        - Rule optimization
        - Detection engine optimization (fast pattern)
    - Auto completion
- In your preferred editors
- Tested with:
    - Visual Studio Code
    - Neovim
    - Kate
    - Sublime Text 3

VS Code


alert.rules - suricata-language-server - Visual Studio Code
File Edit Selection View Go Run Terminal Help
alert.rules 5, U
tests > alert.rules
1 alert tcp any any -> any any (msg:"rer"; content:"rer B"; content:"rer C"; flow:established,to_client; sid:1; rev:1;)
2 #alert http any any -> any any (msg:"next try"; sid:2; content:"devine"; content: "qui"; rev:2;)
3 alert http any any -> any any (msg:"next try"; sid:2; content:"loir"; content:"devine"; content: "qui"; rev:2;)
4 alert ip any any -> any any (msg:"rer"; sid:5; rev:3; flow:established,to_server; http.useragent; content:"toto";)
5 alert rdp any any -> any any (msg:"rdp test"; sid:2; rev: 4;)
6 alert http any any -> any any (msg:"test http"; http.host; content:"TOTO"; sid:10;)
7
PROBLEMS 5 OUTPUT DEBUG CONSOLE TERMINAL
Filter (e.g. text, **/*.ts, !**/node_modules/**)
alert.rules tests 5
unknown rule keyword 'http.useragent'. [6, 1]
TCP rule without a flow or flags option. [3, 48]
Rule is inspecting both the request and the response. [3, 48]
Signature with newer revision, so the older sig replaced by this new signature [5, 47]
A pattern with uppercase chars detected for http_host. Since the hostname buffer we match against is lowercase only, please specify a lowercase pattern. [6, 1]
main* Python 3.10.1 64-bit 1 4 "alert.rules" 7L 589C written
Ln 6, Col 72 Spaces: 4 UTF-8 LF Suricata

Neovim


1., alert.rules (6) ●
1 alert tcp any any → any any (msg:"rer"; content:"rer B"; content:"rer C"; flow:established,to_client; sid:1; rev:1;)
2 #alert http any any → any any (msg:"next try"; sid:2; content:"devine"; content: "qui"; rev:2;)
3 alert http any any → any any (msg:"next try"; sid:2; http.us content:"loir"; content:"devine"; content: "qui"; rev:2;)
Sticky Buffer
http.user_agent Keyword
er; http.user_agent; content:"TOTO";)
rev: 4;) ■ Signature with newer revision, so the older sig replace
sticky buffer to match specifically and only on the
HTTP User Agent buffer
[Documentation](https://suricata.readthedocs.io/en/
latest/rules/http-keywords.html#http-user-agent)

More info

- Suricata Language Server:
  - https://github.com/StamusNetworks/suricata-language-server
  - VS Code plugin: Suricata Intellisense
- Suricata Language Server webinar: https://www.stamus-networks.com/suricata-language-server
- Suricata for Analysts book: https://www.stamus-networks.com/suricata-4-analysts
- Contact me:
  - Twitter: @regiteric
  - Mail: el@stamus-networks.com