Suricata-Update

- A rule update tool for Suricata
- Like Oinkmaster and Pulled Pork
- Opinionated, specifically for Suricata
- Usage and configuration should be familiar to users of existing tools.
Goals

- Just work, without any configuration
- Easy to use
- Become the standard update tool.
- Bundle with Suricata (and it is as of 4.1)
History

- Forked from idstools-rulecat rule update tool
- Officially introduced at SuriCon 2017
- First release, 1.0.0a1, December 2017
- 1.0 final bundled with Suricata 4.1, November 2018
Features

- Update your rules
- Multiple rule sources
- Disable rules
- Enable rules
- Modify rules
- Convert rules to drop
- Test the rules with -T
- Reload Suricata

- Written in Python
- Supports Python 2.7 and 3
- Minimal Dependencies
  - pyyaml
- Suricata configuration aware
- Flowbit dependency resolution
- Suricata Rule Index
Suricata Rule Index
Suricata Rule Index

- A directory of Suricata rulesets
  - Managed by the OISF
- Conceived at SuriCon 2017 (by Victor)
- Make rule sources easier to discover for users
- Allow rule writers to be more discoverable
Current Rulesets

- Emerging Threats Open
- Emerging Threats Pro *
- Abuse.ch SSL Blacklist
- Positive Technologies Attack Detection

- Secureworks Security *
- Secureworks Malware *
- Etnetera Aggressive IP Blacklist
- OISF Traffic ID

* requires paid subscription
Get Listed

- Contact us
  - Email, pull request on index, issue
- Even if experimental
  - Make use of latest and greatest rule features!
# Proofpoint/Emerging Threats Pro ruleset.

**et/pro:**
- **summary:** Emerging Threats Pro Ruleset
- **description:** Proofpoint ET Pro is a timely and accurate rule set for detecting and blocking advanced threats.
- **vendor:** Proofpoint
- **license:** Commercial
- **url:** https://rules.emergingthreatspro.com/%(secret-code)s/suricata-%(__version__)s/etpro.rules.tar.gz
- **subscribe-url:** https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
- **parameters:**
  - **secret-code:**
    - **prompt:** Emerging Threats Pro access code
- **replaces:**
  - et/open

# The OISF Traffic ID ruleset.

**oisd/trafficid:**
- **vendor:** OISF
- **summary:** Suricata Traffic ID ruleset
- **license:** MIT
- **url:** https://raw.githubusercontent.com/jasonish/suricata-trafficid/master/rules/traffic-id.rules
- **support-url:** https://redmine.openinfosecfoundation.org/
- **min-version:** 4.0.0
Back to Suricata-Update
Installation

- Included with Suricata 4.1
- If still using Suricata 4.0:
  - pip install --upgrade suricata-update
- Can also be run from the source directory
  - ./bin/suricata-update
default-rule-path: /var/lib/suricata/rules
rule-files:
- botcc.rules
- botcc.portgrouped.rules
- ciarmy.rules
- compromised.rules
- drop.rules
- dshield.rules
- emerging-activex.rules
- emerging-attack_response.rules
- emerging-chat.rules
- emerging-current_events.rules
- emerging-dns.rules
- emerging-dos.rules
- emerging-exploit.rules
- emerging-ftp.rules
- emerging-games.rules
- emerging-icmp_info.rules
- emerging-icmp.rules
- emerging-imap.rules
- emerging-inappropriate.rules
Prepare Suricata

default-rule-path: /var/lib/suricata/rules
rule-files:
  - suricata.rules
Suricata Provided Rules

Old Location:
/etc/suricata/rules

New Location:
/usr/share/suricata/rules
Basic Usage

$ suricata-update

• Emerging Threats Open used by default.
• Disable any rules required features not enabled (best try)
• Resolve flowbit dependencies
• Write single file, /var/lib/suricata/rules/suricata.rules
Basic Configuration

- /etc/suricata/disable.conf
- /etc/suricata/enable.conf
- /etc/suricata/modify.conf
- /etc/suricata/drop.conf

--sysconfdir respected.
Permissions

- You could just run as root or with sudo...
- Read access to /etc/suricata
- Write access to /var/lib/suricata
- Sudo to SIGUSR2 Suricata
- OR write access to the Suricata control socket
Rule Matching

- **Signature ID**
  - 2019401
  - 1:2019401

- **Regular expression**
  - re:heartbleed
  - re:MS(0[7-9]|10)-\d+

- **Rule group**
  - group:emerging-icmp.rules
  - group:emerging-dos
Rule Modifications

re:classtype:trojan-activity "(alert)(.*)" "drop\2"

modifyisd * "^drop(.*)noalert(.)" | "alert${1}noalert${2}"  
(for those moving over from Oinkmaster)
Other Commands

- **update-sources**
  - Update the source index
  - Also gives the OISF some telemetry
- **list-sources**
  - List available rule sources
- **enable-source**
  - Enable a source found in the index
Other Commands

- **disable-source**
  - Disable a previously enabled source
- **remove-source**
  - Remove a previously disabled source
- **list-enabled-sources**
  - List all enabled sources
- **add-source**
  - Add a custom rule source by URL
Current Issues

- Supporting Python 2 and 3
- A deterministic way to handle duplicate SIDs
- Alternate authentications methods
- Oinkmaster Like Report
- SID allocation
Resources

https://github.com/OISF/suricata-update

https://redmine.openinfosecfoundation.org/projects/suricata-update

https://suricata-update.readthedocs.io/
OISF Traffic ID Ruleset
OISF Traffic ID Ruleset

- SuriCon 2017 Brainstorm Issue #2291
- Identify and label traffic
OISF Traffic ID Ruleset

# Traffic identification where more than one pattern are required.

## Debian APT-GET
- **id**: debian-apt
- **msg**: "Debian APT-GET"
- **labels**:
  - software-update
- **proto**: http
- **http_host**: debian.org
- **http_user_agent**: Debian APT

## TLS SNI patterns

```bash
# TLS SNI patterns.
tls-sni-patterns:

# Facebook.
- **id**: facebook
  - **labels**:
    - social-network
  - **patterns**:
    - facebook.com
    - facebook.net
    - fbcdn.net
    - fbcdn.com
    - fbsbx.com

# Facebook Messenger.
- **id**: facebook-messenger
  - **labels**:
    - im
  - **patterns**:
    - edge-chat.facebook.com
```
alert tls any any -> any any (msg:"SURICATA TRAFFIC-ID: facebook"; 
   tls_sni; content:"facebook.com"; isdataat:!1,relative; 
   flow:to_server,established; \
   flowbits:set,traffic/id/facebook; \ 
   flowbits:set,traffic/label/social-network; \
   noalert; sid:300000001; rev:1;)

"traffic": { 
   "id": [ 
      "facebook" 
   ], 
   "label": [ 
      "social-network" 
   ] 
}
The Future

- Lua Rules & Output Scripts
- Dynamically Loaded Modules
- Meta Profiles
- Expand the Rule Index
- Expand The Traffic ID Ruleset
- Submit Your Ideas