Porkroll – A Snort SO Compiler

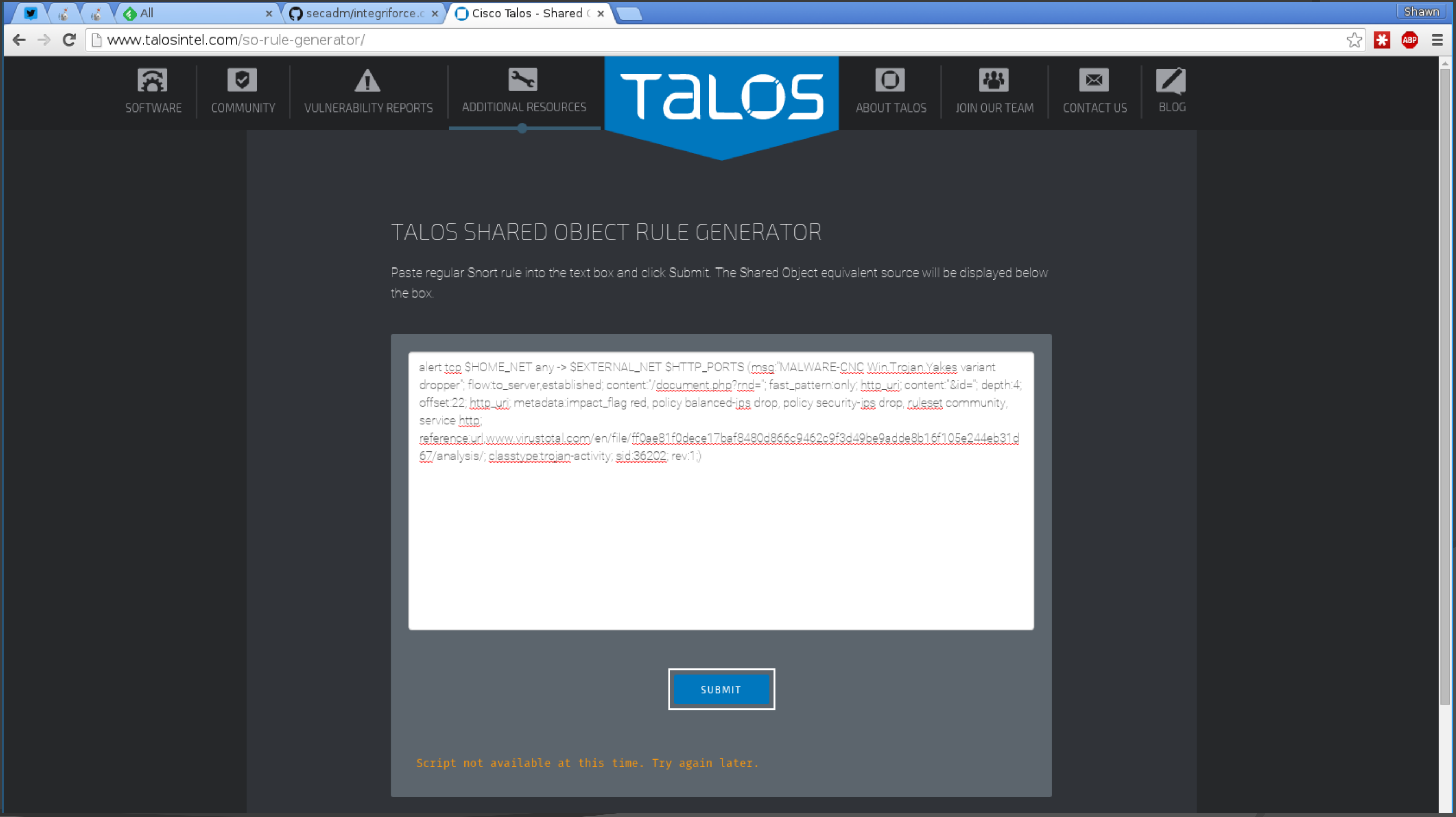
Shawn Webb
G2, Inc

December 2015

Who am I?

- Newb
- Former Cisco Talos employee
- Current employee of G2, Inc
- Security engineer
- Cofounder of HardenedBSD
- FreeBSD and HardenedBSD fanboy
- Lover of ZFS and Dtrace
- Opensource enthusiast

What and Why?



TALOS SHARED OBJECT RULE GENERATOR

Paste regular Snort rule into the text box and click Submit. The Shared Object equivalent source will be displayed below the box.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.Yakes variant dropper"; flow:to_server,established; content:"/document.php?rnd="; fast_pattern:only; http_uri; content:"&id="; depth:4; offset:22; http_uri; metadata:impact_flag red, policy balanced-ips drop, policy security-ips drop, ruleset community, service http; reference:url,www.virustotal.com/en/file/ff0ae81f0dece17baf8480d866c9462c9f3d49be9adde8b16f105e244eb31d67/analysis/; classtype:trojan-activity; sid:36202; rev:1;)
```

SUBMIT

```
Script not available at this time. Try again later.
```

What and why?

- Customer can't use plaintext rules, requires Snort Shared Object (aka, SO) rules
- Cisco Talos already has a nifty tool
  - Web form only
  - Screen scrape?
  - Only produces C code, not deployable SO
- Takes a plaintext Snort rule json object (lolwut?)
  - Converts it to a fully-deployable SO
  - Automation!

https://gist.github.com/j105rob/1341bfc44c32c00c3a0a

Moar JSON!

- Parsing Snort rules is hard
- Too difficult to do in zsh, python needed
- I suck at regex
- Coworker, Rob Weiss, wrote:

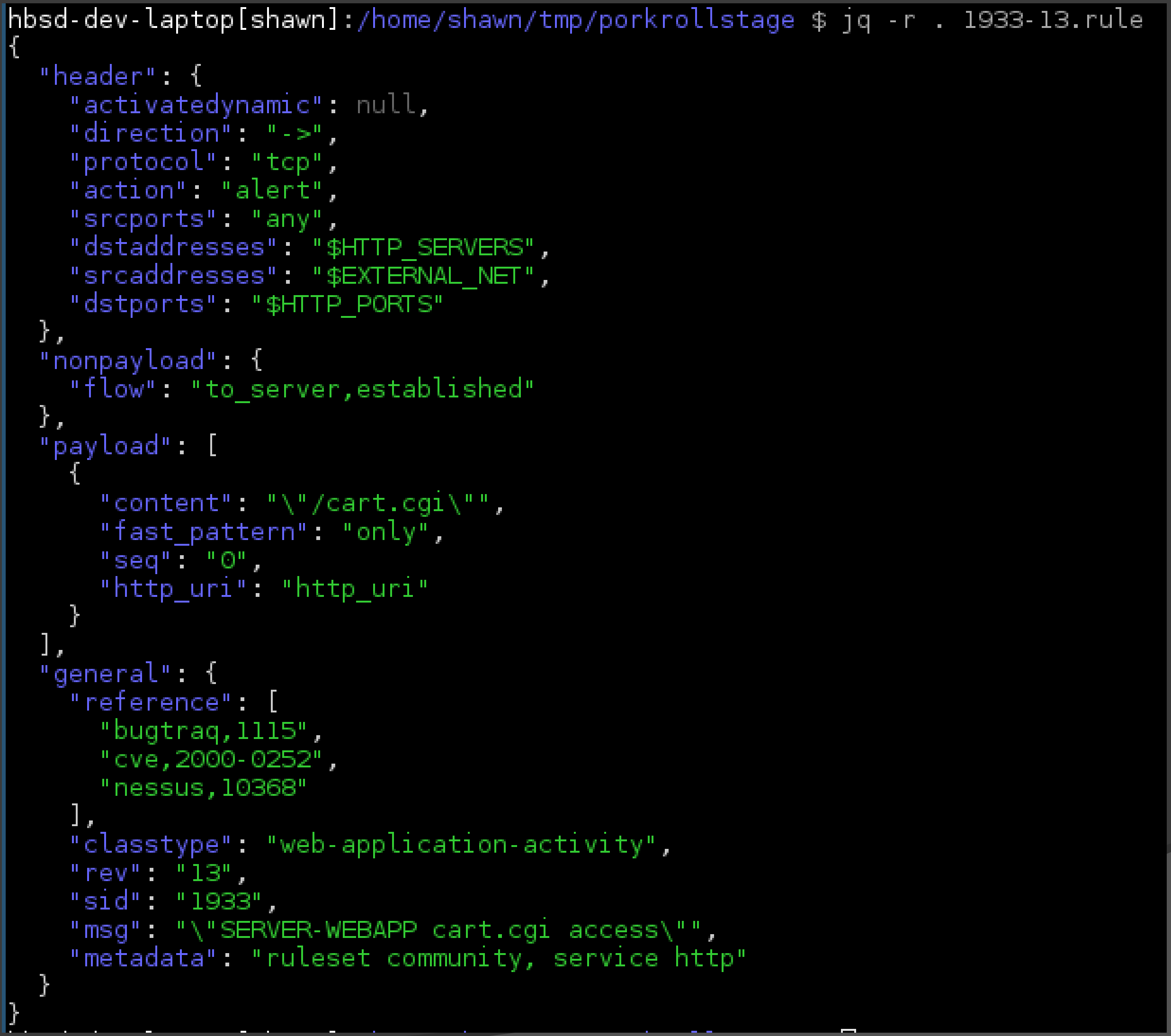
  https://gist.github.com/j105rob/1341bfc44c32c00c3a0a

- Official project will happen soon
- May integrate with PulledPork

Example Snort Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"MALWARE-CNC Win.Trojan.Kovtar outbound connection";
flow:to_server,established; content:"/counter/?id="; fast_pattern:only; http_uri;
content:"&rnd="; offset:13; http_uri; content:"UA-CPU"; http_header;
metadata:impact_flag red, policy balanced-ips drop, policy security-ips drop,
ruleset community, service http;
reference:url,www.virustotal.com/en/file/9d6b1bd74848dd0549ad3883b7292d3ba
0a4fa06d0aaf562032b0bf6dc198249/analysis/; classtype:trojan-activity;
sid:37045; rev:1;)
```

Example JSON Snort Rule



```
hbsd-dev-laptop[shawn]:/home/shawn/tmp/porkrollstage $ jq -r . 1933-13.rule
{
  "header": {
    "activatedynamic": null,
    "direction": "->",
    "protocol": "tcp",
    "action": "alert",
    "srcports": "any",
    "dstaddresses": "$HTTP_SERVERS",
    "srcaddresses": "$EXTERNAL_NET",
    "dstports": "$HTTP_PORTS"
  },
  "nonpayload": {
    "flow": "to_server,established"
  },
  "payload": [
    {
      "content": "\"/cart.cgi\"",
      "fast_pattern": "only",
      "seq": "0",
      "http_uri": "http_uri"
    }
  ],
  "general": {
    "reference": [
      "bugtraq,1115",
      "cve,2000-0252",
      "nessus,10368"
    ],
    "classtype": "web-application-activity",
    "rev": "13",
    "sid": "1933",
    "msg": "\"SERVER-WEBAPP cart.cgi access\"",
    "metadata": "ruleset community, service http"
  }
}
```

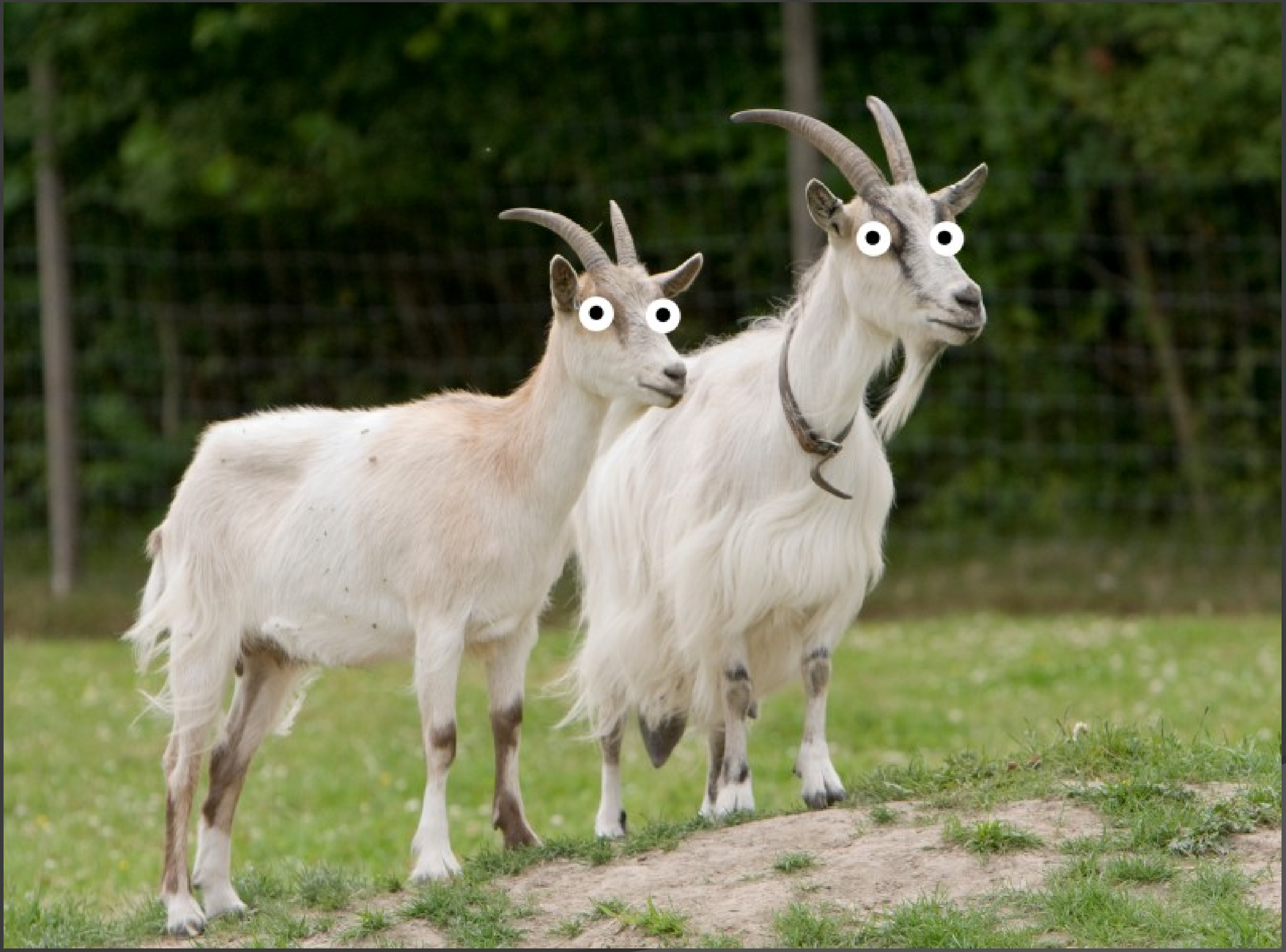
Compilation Steps

- JSONify rules
  - One rule per JSON file
- Run Porkroll:
  - Untar snort source code
  - Inspect each JSON rule
  - Output C source code matching the JSON object
  - Tie in to Snort build scripts
  - Re-run autotools
  - ./configure; make

TODO

- More complex rules
  - Lots of keywords not implemented
- Integration with PulledPork
  - Get rid of the JSONification
- Create Snort .stub file
- Launch in production

Demo



Questions

Porkroll Team:

Shawn Webb
Security Engineer
shawn.webb@g2-inc.com

Rob Weiss
SME
rob.weiss@g2-inc.com

Stephen Pietrasko
Security Engineer
stephen.pietrasko@g2-inc.com

https://github.com/lattera/porkroll