The Bro Package Manager and You

Seth Hall
Chief Evangelist
Corelight, Inc

About Me

Bro at all of them!

-  - Incident Responder
-  - Detection-Response Architect
-  - **Core Bro developer**
-  - **Co-founder & Chief Evangelist**

Funded by

aux/plugins?

bro / bro-plugins

Unwatch 21 | Star 54 | Fork 33

Code | Pull requests 0 | Settings | Insights

Plugins for Bro

Edit

Add topics

200 commits | 4 branches | 6 releases | 17 contributors

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

sethhall Grammatical fixes. Latest commit 3ceeedd a minute ago

README Grammatical fixes. a minute ago

README

NOTE: We no longer maintain any Bro plugins here. Most of the
plugins that used to be available here have been moved over to use the
Bro Package Manager instead. See https://github.com/bro/packages for a
list of Bro packages currently available.

aux/plugins?

bro / bro-plugins

Unwatch 21 | Star 54 | Fork 33

Code | Pull requests 0 | Settings | Insights

Plugins for Bro

Edit

Add topics

200 commits | 4 branches

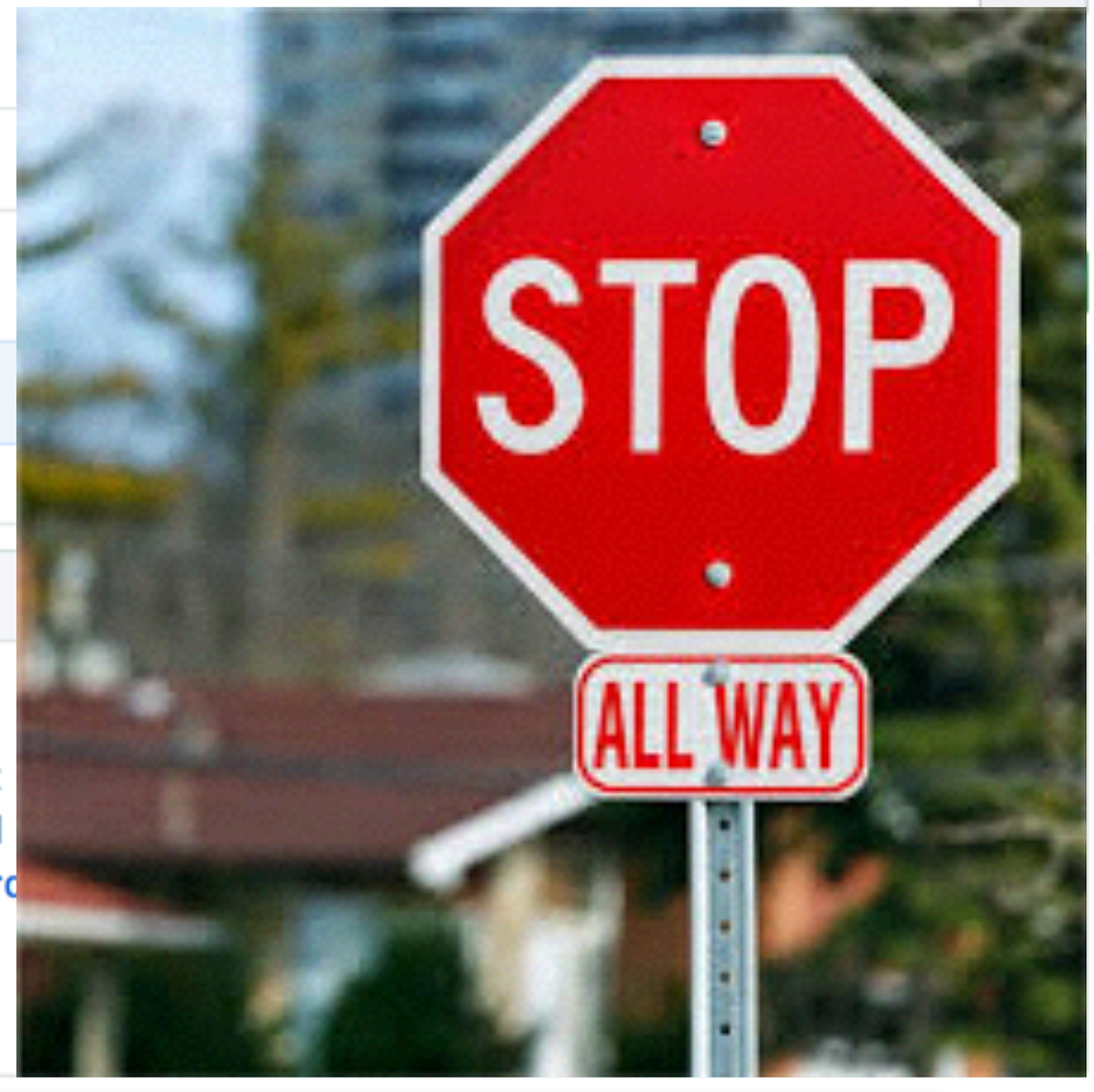
Branch: master | New pull request

sethhall Grammatical fixes.

README Grammatical fixes.

README

NOTE: We no longer maintain any Bro plugins here. Most
plugins that used to be available here have been moved
Bro Package Manager instead. See https://github.com/bro
list of Bro packages currently available.



Simple to install

$ sudo pip install bro-pkg

More complete docs…
http://bro-package-manager.readthedocs.io/en/stable/quickstart.html

Configure and Integrate

- If Bro isn’t in your path…
  - $ export PATH=/opt/bro/bin/:$PATH
- $ mkdir ~/.bro-pkg
- $ bro-pkg autoconfig > ~/.bro-pkg/config
- **@load packages**
- **You may need to deal with some permission issues, but it’s documented! Please take a look at the docs!**

Bundles for DevOps

```
$ bro-pkg bundle my-stuff.bundle
```

Move my-stuff.bundle over to another machine...

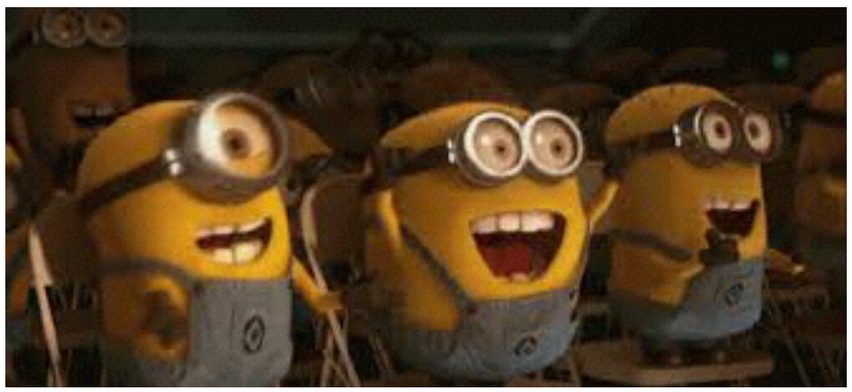
```
$ bro-pkg unbundle my-stuff.bundle
```

Bundles for DevOps

```
$ bro-pkg bundle my-stuff.bundle
```

Move my-stuff.bundle over to another machine...

```
$ bro-pkg unbundle my-stuff.bundle
```



What’s out there?

- **Update the local list of global packages**
  - $ bro-pkg refresh
- **Get the list of packages**
  - $ bro-pkg list all

What's out there?

bro/0xxon/bro-postgresql
bro/0xxon/bro-sumstats-counttable
bro/corelight/bro-drwatson
bro/corelight/bro-hardware
bro/corelight/bro-long-connections
bro/corelight/bro-shellshock
bro/corelight/bro-xor-exe-plugin
bro/corelight/top-dns
bro/dopheide/bro_notice_correlation
bro/dopheide/venom
bro/hhzzk/dns-tunnels
bro/hosom/file-extraction
bro/hosom/log-filters
bro/initconf/CVE-2017-5638_struts
bro/initconf/CVE-2017-5638_struts.git
bro/initconf/phish-analysis
bro/initconf/scan-NG
bro/initconf/smtp-url-analysis
bro/j-gras/add-json
bro/j-gras/bro-af_packet-plugin
bro/j-gras/bro-lognorm
bro/j-gras/intel-extensions
bro/joesecurity/Joe-Sandbox-Bro
bro/jonzeolla/scan-sampling
bro/jsiwek/bro-test-package
bro/jswaro/tcprs
bro/ncsa/bro-doctor
bro/ncsa/bro-interface-setup
bro/ncsa/bro-is-darknet
bro/ncsa/bro-simple-scan
bro/pgaulon/bro-notice-slack
bro/scebro/ldap-analyzer
bro/sethhall/bro-brainfuck
bro/sethhall/bro-myricom
bro/sethhall/credit-card-exposure
bro/sethhall/domain-tld
bro/sethhall/ssn-exposure
bro/sethhall/unknown-mime-type-discovery
bro/srozb/dns_axfr
bro/theflakes/bro-large_uploads

What's out there?

40 Packages!

bro/0xxon/bro-postgresql
bro/0xxon/bro-sumstats-counttable
bro/corelight/bro-drwatson
bro/corelight/bro-hardware
bro/corelight/bro-long-connections
bro/corelight/bro-shellshock
bro/corelight/bro-xor-exe-plugin
bro/corelight/top-dns
bro/dopheide/bro_notice_correlation
bro/dopheide/venom
bro/hhzzk/dns-tunnels
bro/hosom/file-extraction
bro/hosom/log-filters
bro/initconf/CVE-2017-5638_struts
bro/initconf/CVE-2017-5638_struts.git
bro/initconf/phish-analysis
bro/initconf/scan-NG
bro/initconf/smtp-url-analysis
bro/j-gras/add-json
bro/j-gras/bro-af_packet-plugin
bro/j-gras/bro-lognorm
bro/j-gras/intel-extensions
bro/joesecurity/Joe-Sandbox-Bro
bro/jonzeolla/scan-sampling
bro/jsiwek/bro-test-package
bro/jswaro/tcprs
bro/ncsa/bro-doctor
bro/ncsa/bro-interface-setup
bro/ncsa/bro-is-darknet
bro/ncsa/bro-simple-scan
bro/pgaulon/bro-notice-slack
bro/scebro/ldap-analyzer
bro/sethhall/bro-brainfuck
bro/sethhall/bro-myricom
bro/sethhall/credit-card-exposure
bro/sethhall/domain-tld
bro/sethhall/ssn-exposure
bro/sethhall/unknown-mime-type-discovery
bro/srozb/dns_axfr
bro/theflakes/bro-large_uploads

corelight/bro-long-connections

New log: conn_long.log

$ bro-pkg install corelight/bro-long-connections

joesecurity/Joe-Sandbox-Bro

Upload files to a JOE Sandbox

$ bro-pkg install joesecurity/Joe-Sandbox-Bro

Configuration?!

```
6   module JoeSandbox;
7
8   export {
9       ##########################
10      #     Settings           #
11      ##########################
12
13      # Joe Sandbox api key
14      const apikey: string = "YOUR_API_KEY" &redef;
15
16      # Joe Sandbox api url
17      # const apiurl: string = "http://example.net/joesandbox/index.php/api/";
18      const apiurl: string = "https://jbxcloud.joesecurity.org/api/" &redef;
19
20      # Please accept the Joe Sandbox Cloud Terms and Conditions if you are
21      # using Joe Sandbox Cloud.
22      # https://jbxcloud.joesecurity.org/download/termsandconditions.pdf
23      const accept_tac: bool = F &redef;
24
```

sethhall/unknown-mime-type-discovery

New log: unknown_mime_type_discovery.log

$ bro-pkg install sethhall/unknown-mime-type-discovery

ncsa/bro-doctor

BroCtl plugin to help diagnose problems

$ bro-pkg install ncsa/bro-doctor

pgaulon/bro-notice-slack

Notice action to send notices to Slack.

$ bro-pkg install pgaulon/bro-notice-slack

Future

Rethink how configuration works

Bro Package Manager website

Rethinking how parts of Bro are distributed

http://bro-package-manager.readthedocs.io/en/stable/

(or type “bro package manager” into google)