

Bro Package Manager

Why aren't scripts being shared?

- Secret techniques?
- Organizational momentum against sharing?
- Difficulty in making scripts generally applicable?
- **Difficulty in discovery and installation?**

We can solve this one!

Thanks!

mozilla

What's the idea?

- Like Python's pip or Ruby gems
- Make it easy to connect script authors with script users
- Foster an ecosystem of shared scripts to improve everyone
 - Nice side effect of making life a tiny bit hard on attackers

Design and Architecture

- Python library with a command line frontend
- Centralized package repository but possible to configure others
- Low friction for contributions
- Not packages with Bro or tied to Bro's release schedule



Requirement: Bro 2.5

Installation



pip install bro-pkg

☰ 1. Quickstart Guide

1.1. Dependencies

1.2. Installation

1.3. Basic Configuration

1.4. Advanced Configuration

1.5. Usage

2. bro-pkg Command-Line Tool

3. How-To: Create a Package

4. How-To: Create a Package Source

5. Python API Reference

6. Developer's Guide

1. Quickstart Guide

1.1. Dependencies

- Python 2.7+ or 3.0+
- git: <https://git-scm.com>
- GitPython: <https://pypi.python.org/pypi/GitPython>
- semantic_version: https://pypi.python.org/pypi/semantic_version

Note that following the suggested [Installation](#) process via **pip** will automatically install *GitPython* and *semantic_version* for you.

1.2. Installation

Using the latest stable release on [PyPI](#):

```
$ pip install bro-pkg
```

Using the latest git development version:

```
$ pip install git+git://github.com/bro/package-manager@master
```

Configuration

If “bro” isn’t in your path, first do.....

```
$ export PATH=/opt/bro/bin/:$PATH
```

Then...

```
$ mkdir -p ~/.bro-pkg
```

```
$ bro-pkg autoconfig > ~/.bro-pkg/config
```

You are configuring a
user account to use
bro-pkg!

You might have permissions trouble!

```
[user@server ~]$ bro-pkg install ssn-exposure
```



```
OSError: [Errno 13] Permission denied: '/usr/local/bro/share/bro/site/packages'
```

```
error: user does not have write access in /usr/local/bro/share/bro/site
```

```
error: user does not have write access in /usr/local/bro/lib/bro/plugins
```

This happened because it's installing into
your installed Bro directories

Loading scripts

@load packages

Add that to local.bro or
load it from the
command line



Package list

```
[user@server ~]$ bro-pkg list all  
bro/broala/bro-long-connections (installed)  
bro/jsiwek/bro-test-package  
bro/sethhall/credit-card-exposure (installed)  
bro/sethhall/ssn-exposure (installed)
```

Searching

```
[user@server ~]$ bro-pkg search dlp
bro/sethhall/credit-card-exposure
  tags: file analysis, credit card, cc, dlp, data loss
bro/sethhall/ssn-exposure
  tags: file analysis, social security number, ssn, dlp, data loss
```

Some other commands

If a package causes trouble, remove it!

```
[user@server ~]$ bro-pkg remove ssn-exposure  
removed "ssn-exposure"
```

Maybe you just want to unload it

```
[seth@Blake tmp]$ bro-pkg unload ssn-exposure  
unloaded "ssn-exposure"
```

Update packages

```
[user@server ~]$ bro-pkg upgrade --all
```

Making Packages

- Packages are just git repositories
- Only need a single file to describe the package (bro-pkg.meta)
- And it's a simple file!

Let's go make one!

Create a repository

sethall / domain-tld

Unwatch1

Star0

Fork0

Code

Issues0

Pull requests0

Wiki

Pulse

Graphs

Settings

Bro script library for getting the effective TLD of a domain. — Edit

2 commits

1 branch

0 releases

1 contributor

BSD-3-Clause

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download

sethall

Tiny rewording to README text

Latest commit 9064ae5 8 hours ago

aux	Initial commit.	9 hours ago
scripts	Initial commit.	9 hours ago
COPYING	Initial commit.	9 hours ago
README.rst	Tiny rewording to README text	8 hours ago
bro-pkg.meta	Initial commit.	9 hours ago

README.rst

Add a bro-pkg.meta

Branch: master ▼

[ssn-exposure](#) / bro-pkg.meta

Find file

Copy path



seth hall Turned into a Bro package.

0f44123 2 days ago

1 contributor

4 lines (3 sloc) | 47 Bytes

Raw


Blame

History



```
1 [package]
2 version = 1.0.0
3 script_dir = scripts
```

Fork the packages repository

 **bro / packages**

Unwatch 6

Star 2

Fork 1

<> Code

Issues 0

Pull requests 0

Wiki

Pulse

Graphs

Settings

The default package source of the Bro Package Manager: <https://github.com/bro/package-manager> — Edit

12 commits

1 branch

0 releases

2 contributors

Branch: master ▾


New pull request





Create new file

Upload files


Find file




Clone or download ▾

 **seth hall** Adding the domain-tld library. Latest commit 335a698 9 hours ago

 broala	Changing the name back since bro-pkg doesn't care.	11 days ago
 jsiwek	Switch to using package index files.	a month ago
 seth hall	Adding the domain-tld library.	9 hours ago
 README.rst	Clarify submission process.	28 days ago


Add it to the main package repo

 **sethhall / packages**
forked from [bro/packages](#)




 Unwatch ▾ 1  Star 0  Fork 1

[Code](#) [Pull requests 0](#) [Wiki](#) [Pulse](#) [Graphs](#) [Settings](#)

Branch: master ▾ **packages / setthall / bro-pkg.index** [Find file](#) [Copy path](#)

 **sethhall** Added credit-card-exposure as a package. bf91efe 13 days ago


1 contributor

4 lines (3 sloc) 132 Bytes [Raw](#) [Blame](#) [History](#)   

```
1 [credit-card-exposure]
2 url = https://github.com/setthall/credit-card-exposure
3 tags = file analysis, credit card, cc, dlp, data loss
```


Submit a pull request

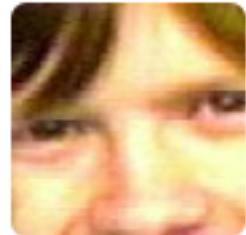
Added credit-card-exposure as a package. #2

 **Merged** **sethall** merged 1 commit into `bro:master` from `sethall:master` 13 days ago

 Conversation **0**



 Commits **1**

 Files changed **1**



sethall commented 13 days ago

New package and adding a directory for me!

  Added credit-card-exposure as a pack



 **sethall** merged commit **1c12483** into `bro:master` 13 days ago

Revert

And get it merged!

Future Directions

- Dependencies
- Testing and linting infrastructure
- More automation on the backend for managing the packages repo
- More packages!

<http://bro-package-manager.readthedocs.io>