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

- 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:

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

Using the latest git development version:

```bash
$ 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/setthall/credit-card-exposure (installed)
bro/setthall/ssn-exposure (installed)
Searching

[user@server ~]$ bro-pkg search dlp
bro/setthall/credit-card-exposure
  tags: file analysis, credit card, cc, dlp, data loss
bro/setthall/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

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

Latest commit 9064ae5 8 hours ago

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
<th>Latest Commit</th>
</tr>
</thead>
<tbody>
<tr>
<td>aux</td>
<td>Initial commit.</td>
<td>9 hours ago</td>
</tr>
<tr>
<td>scripts</td>
<td>Initial commit.</td>
<td>9 hours ago</td>
</tr>
<tr>
<td>COPYING</td>
<td>Initial commit.</td>
<td>9 hours ago</td>
</tr>
<tr>
<td>README.rst</td>
<td>Tiny rewording to README text</td>
<td>8 hours ago</td>
</tr>
<tr>
<td>bro-pkg.meta</td>
<td>Initial commit.</td>
<td>9 hours ago</td>
</tr>
<tr>
<td>README.rst</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Add a bro-pkg.meta

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4 lines (3 sloc)</td>
<td>47 Bytes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>package</td>
<td>version = 1.0.0</td>
<td>script_dir = scripts</td>
<td></td>
</tr>
</tbody>
</table>
Fork the packages repository

The default package source of the Bro Package Manager: https://github.com/bro/package-manager — Edit
Add it to the main package repo

[credit-card-exposure]
url = https://github.com/sethhall/credit-card-exposure
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!

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

And get it merged!
Future Directions

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