Who am I?

- Gavin Henry, 43
- CIO of TelcoSwitch
- Founder of SureVoIP (Acquired July 2021)
- Software Engineer
- Software Engineering Radio Podcast Host

SentryPeer

What is SentryPeer?

- An idea
- A side project
- A work in progress
- A distributed list of bad IP addresses
- A distributed list of phone numbers
- All collected via a SIP Honeypot
- A learning project for me

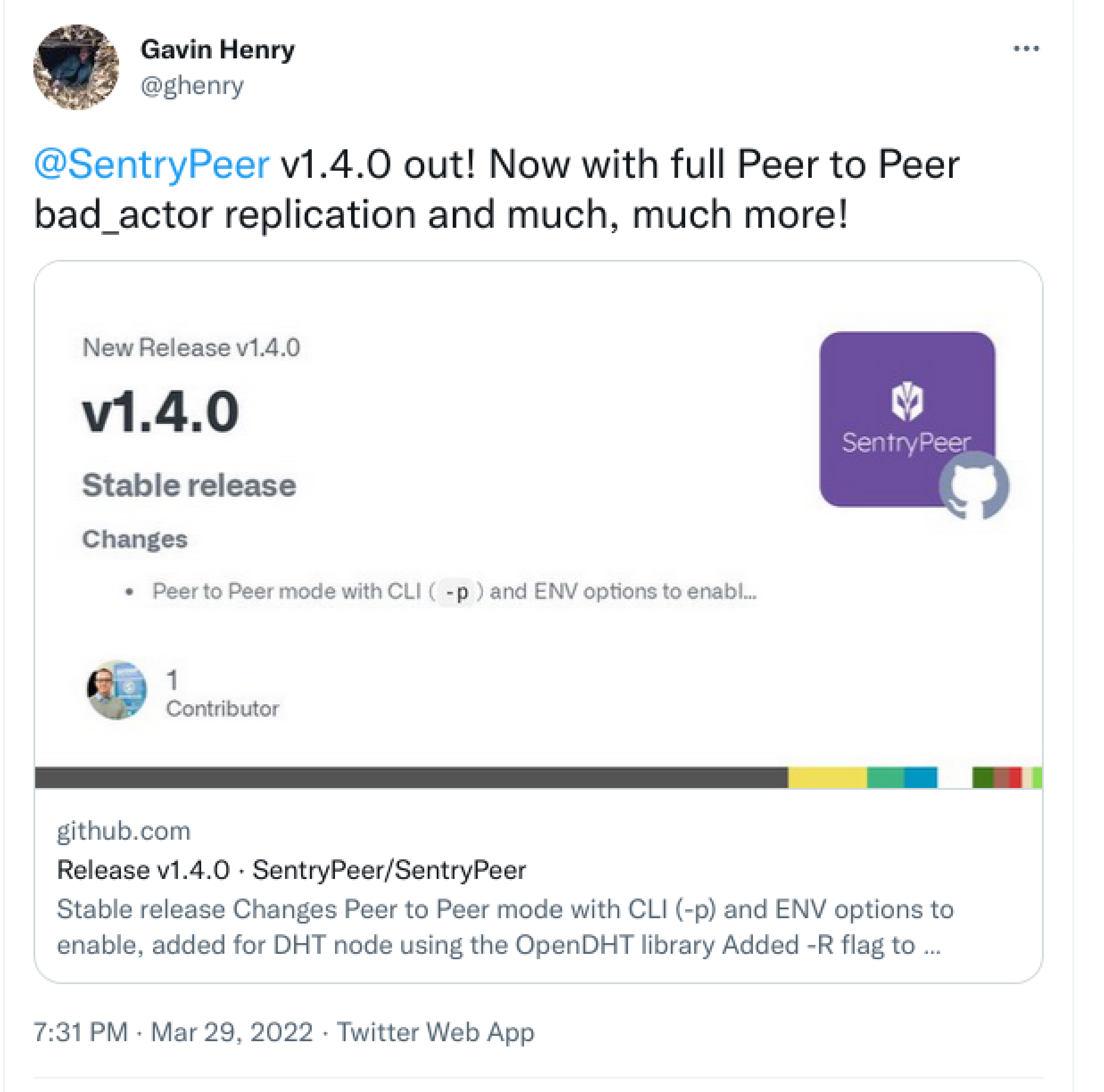
SentryPeer

Why is it different?

- The whole thing is open source
- You own the data
- You can share that data
- You can receive other users data
- It’s Peer to Peer (uses a DHT)
- Best effort Bad Actor replication
- Various agents for using that data
- You run it!

SentryPeer

Peer to Peer release date



Gavin Henry
@ghenry

@SentryPeer v1.4.0 out! Now with full Peer to Peer bad_actor replication and much, much more!

New Release v1.4.0

v1.4.0

Stable release

Changes

- Peer to Peer mode with CLI (`-p`) and ENV options to enabl...

1
Contributor

github.com
Release v1.4.0 · SentryPeer/SentryPeer
Stable release Changes Peer to Peer mode with CLI (-p) and ENV options to enable, added for DHT node using the OpenDHT library Added -R flag to ...

7:31 PM · Mar 29, 2022 · Twitter Web App

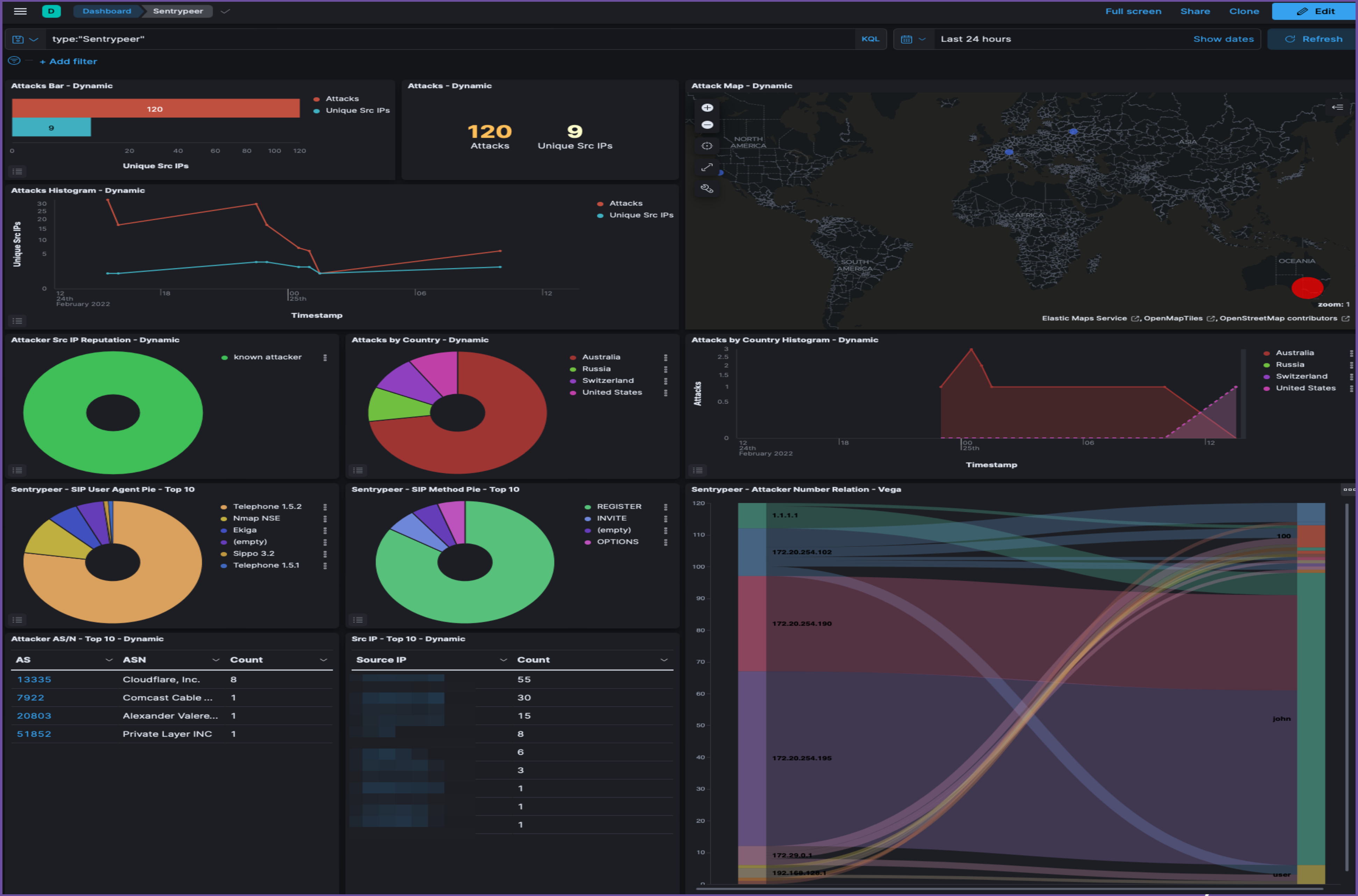
SentryPeer

Tech

- Written in C
- Adopted by Deutsche Telokom T-Pot HoneyPot Project
- Adopted by Kali Linux
- Uses libosip2 with more protocols...
- Hosted on GitHub with lots of Actions
- Uses sqlite
- Uses OpenDHT for Peer to Peer
- Web GUI and REST API
- BGP and SIP endpoints (TBC)

SentryPeer

T-Pot Dashboard



Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
13335	Cloudflare, Inc.	8
7922	Comcast Cable ...	1
20803	Alexander Valere...	1
51852	Private Layer INC	1

Src IP - Top 10 - Dynamic

Source IP	Count
[redacted]	55
[redacted]	30
[redacted]	15
[redacted]	8
[redacted]	6
[redacted]	3
[redacted]	1
[redacted]	1
[redacted]	1

Bad Actor Replication

```
Source IP: 141.98.10.78
Called Number: 800046812111828
SIP Method: INVITE
Transport Type: UDP
User Agent: NOT_FOUND
Collected Method: responsive
Created by Node Id: 6a84307e-1a9c-4ed2-99a7-f538dd28a1b8

SentryPeer db file location is: sentrypeer.db

Saving bad actor to the DHT…

Bad actor in JSON format: {"app_name":"sentrypeer","app_version":"1.4.0","event_timestamp":"2022-03-25
14:07:42.770403209","event_uuid":"ac9f2ebd-d180-48c9-a10f-946a8cfc2a6f","created_by_node_id":"6a84307e-1a9c-
4ed2-99a7-
f538dd28a1b8","collected_method":"responsive","transport_type":"UDP","source_ip":"141.98.10.78","destination_ip":"x.
x","called_number":"800046812111828","sip_method":"INVITE","sip_user_agent":"NOT_FOUND","sip_message":"xx”}

Node ID from DHT value is: 6a84307e-1a9c-4ed2-99a7-f538dd28a1b8
Node ID from DHT value is the same as ours. Not saving bad_actor.
Done callback. Success!
```

SentryPeer

Tech (cont’d)

- Multithreaded
- Syslog for Fail2Ban
- Container on Docker Hub
- All options configurable via ENV
- Homebrew version
- Debian, Ubuntu, Alpine Linux and Fedora packages
- Monthly releases

SentryPeer

JSON logging

```
{
   "app_name":"sentrypeer",
   "app_version":"v1.2.0",
   "event_timestamp":"2022-0-22 11:19:15.848934346",
   "event_uuid":"4503cc92-26cb-4b3e-bb33-69a83fa09321",
   "created_by_node_id":"4503cc92-26cb-4b3e-bb33-69a83fa09321",
   "collected_method":"responsive",
   "transport_type":"UDP",
   "source_ip":"45.134.144.128",
   "destination_ip":"XX.XX.XX.XX",
   "called_number":"0046812118532",
   "sip_method":"OPTIONS",
   "sip_user_agent":"friendly-scanner",
   "sip_message":"full SIP message"
}
```

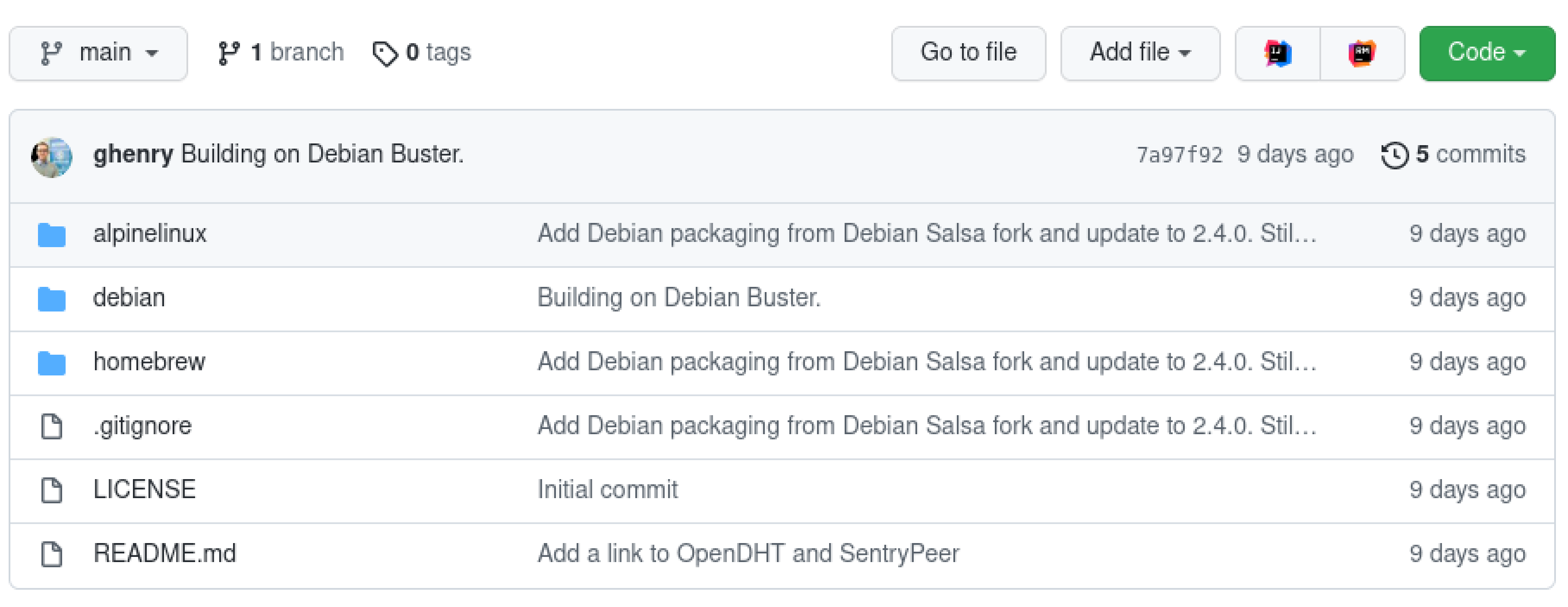
SentryPeer

Network Topology

- Bootstrapping required for Peer to Peer – bootstrap.sentrypeer.org
- Share only to your own nodes
- Various configuration options to enable and disable features
- Terraform recipes

SentryPeer

Yak Shaving

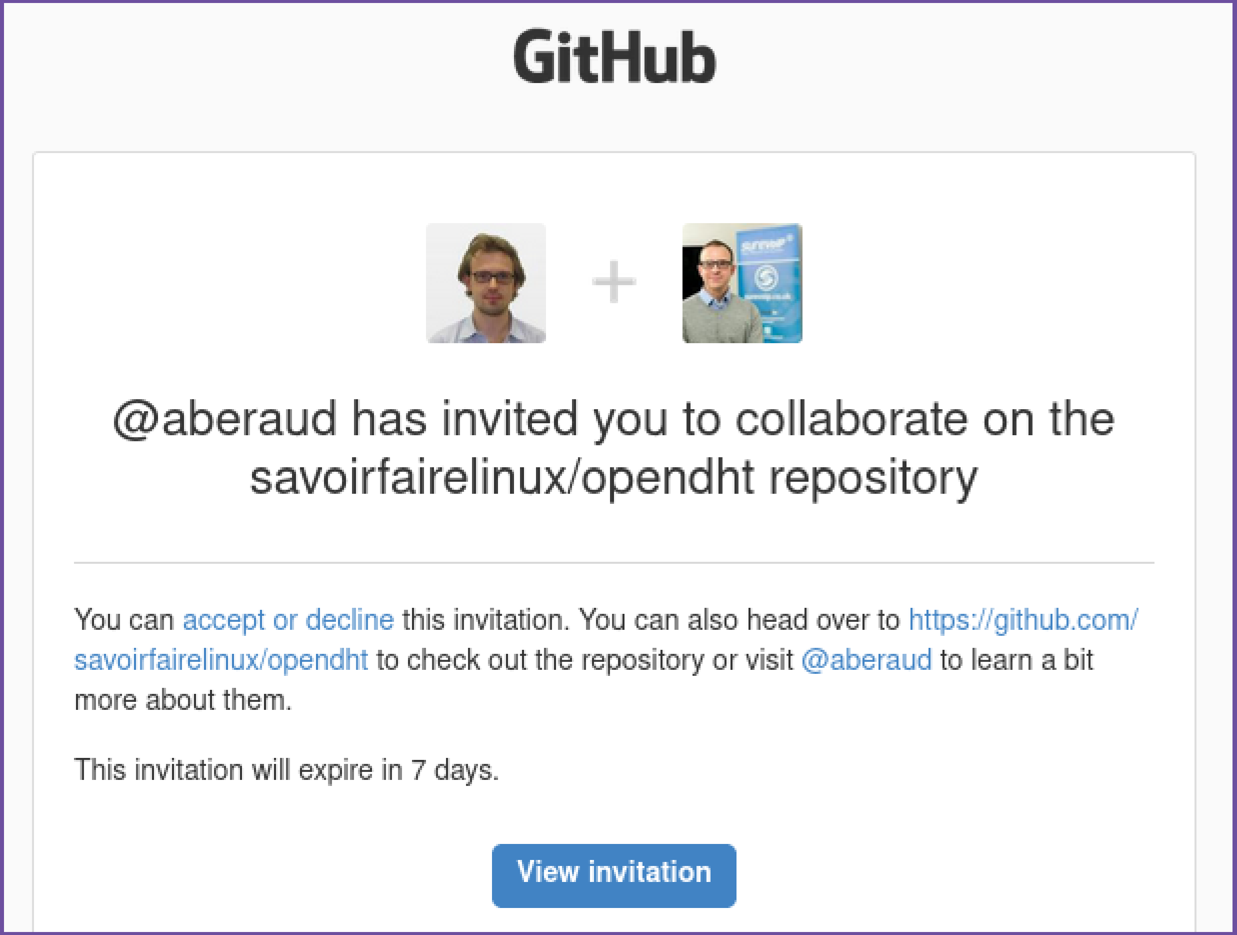


ghenry Building on Debian Buster. 7a97f92 9 days ago **5** commits

alpinelinux	Add Debian packaging from Debian Salsa fork and update to 2.4.0. Stil…	9 days ago
debian	Building on Debian Buster.	9 days ago
homebrew	Add Debian packaging from Debian Salsa fork and update to 2.4.0. Stil…	9 days ago
.gitignore	Add Debian packaging from Debian Salsa fork and update to 2.4.0. Stil…	9 days ago
LICENSE	Initial commit	9 days ago
README.md	Add a link to OpenDHT and SentryPeer	9 days ago

SentryPeer

Unexpected Collaboration



GitHub

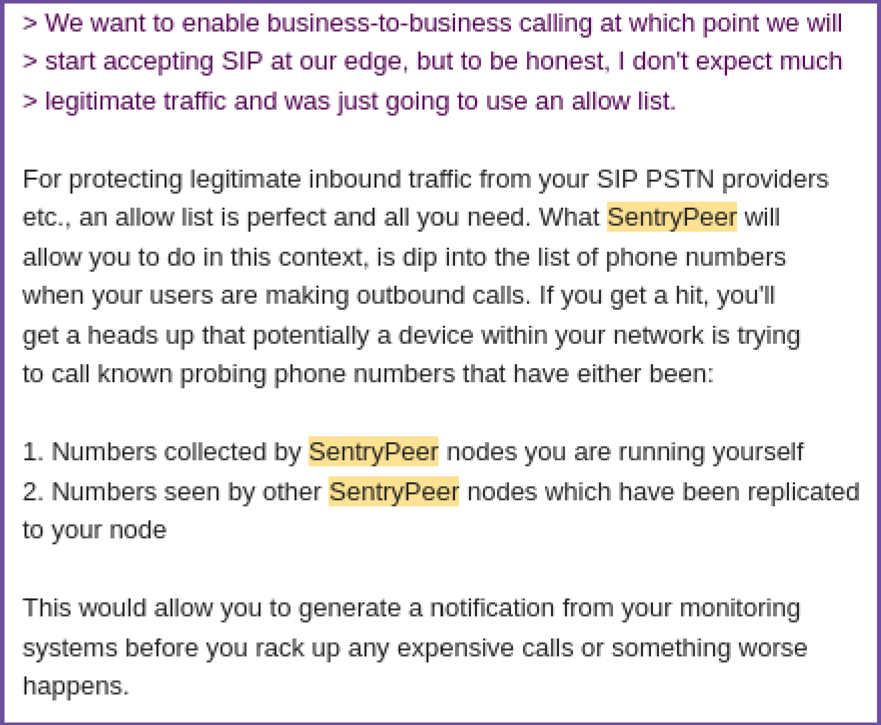
@aberaud has invited you to collaborate on the savoirfairelinux/opendht repository

You can accept or decline this invitation. You can also head over to https://github.com/savoirfairelinux/opendht to check out the repository or visit @aberaud to learn a bit more about them.

This invitation will expire in 7 days.

SentryPeer

Unexpected Community

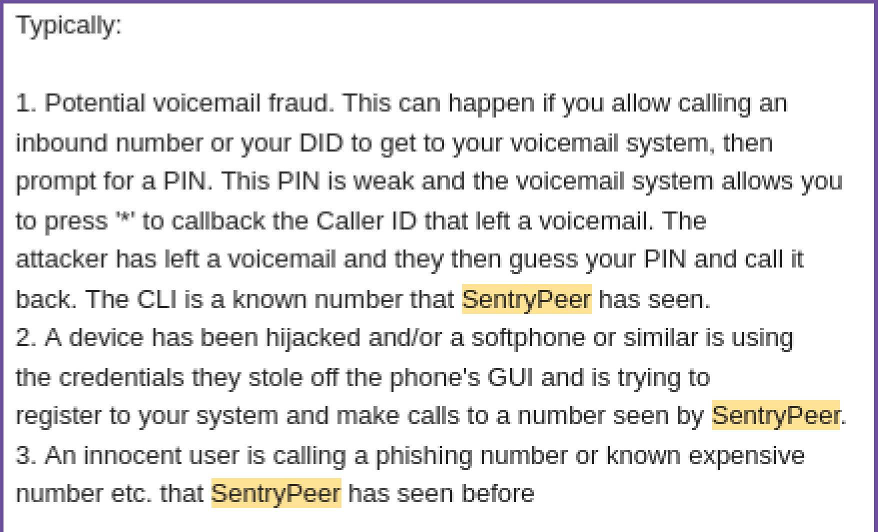


> We want to enable business-to-business calling at which point we will
> start accepting SIP at our edge, but to be honest, I don't expect much
> legitimate traffic and was just going to use an allow list.

For protecting legitimate inbound traffic from your SIP PSTN providers etc., an allow list is perfect and all you need. What SentryPeer will allow you to do in this context, is dip into the list of phone numbers when your users are making outbound calls. If you get a hit, you'll get a heads up that potentially a device within your network is trying to call known probing phone numbers that have either been:

1. Numbers collected by SentryPeer nodes you are running yourself
2. Numbers seen by other SentryPeer nodes which have been replicated to your node

This would allow you to generate a notification from your monitoring systems before you rack up any expensive calls or something worse happens.



Typically:

1. Potential voicemail fraud. This can happen if you allow calling an inbound number or your DID to get to your voicemail system, then prompt for a PIN. This PIN is weak and the voicemail system allows you to press '*' to callback the Caller ID that left a voicemail. The attacker has left a voicemail and they then guess your PIN and call it back. The CLI is a known number that SentryPeer has seen.
2. A device has been hijacked and/or a softphone or similar is using the credentials they stole off the phone's GUI and is trying to register to your system and make calls to a number seen by SentryPeer.
3. An innocent user is calling a phishing number or known expensive number etc. that SentryPeer has seen before

Contribute!

Special thanks to David Miller for our logo, Web gui and colour scheme!

- https://twitter.com/SentryPeer
- https://github.com/SentryPeer/SentryPeer
- https://sentrypeer.org

SentryPeer