Who am I?

• Gavin Henry, 43
• CIO of TelcoSwitch
• Founder of SureVoIP (Acquired July 2021)
• Software Engineer
• Software Engineering Radio Podcast Host
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
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!
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)
T-Pot Dashboard
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.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!
Tech (cont’d)

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

```json
{
    "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"
}
```
Network Topology

- Bootstrapping required for Peer to Peer – bootstrap.sentrypeer.org
- Not needed on your own LAN
- Share only to your own nodes
- Various configuration options to enable and disable features
- Terraform recipes
Results

- Prototype got hits within 20 minutes on a brand new IP address

- Learning sooo much!!! (that’s the other reason I’m doing all this)
Results

- Prototype couldn’t keep up with data stream
# SIP Honeypot Data

Data collected between 17:00 and 18:00 UTC

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.63.64.190</td>
<td>1576481</td>
</tr>
<tr>
<td>141.94.139.30</td>
<td>125</td>
</tr>
<tr>
<td>193.46.255.243</td>
<td>125</td>
</tr>
<tr>
<td>23.148.145.28</td>
<td>125</td>
</tr>
<tr>
<td>40.86.206.158</td>
<td>125</td>
</tr>
<tr>
<td>51.104.46.51</td>
<td>125</td>
</tr>
<tr>
<td>104.149.156.10</td>
<td>125</td>
</tr>
<tr>
<td>92.118.63.42</td>
<td>125</td>
</tr>
<tr>
<td>104.149.141.122</td>
<td>125</td>
</tr>
<tr>
<td>23.148.145.212</td>
<td>125</td>
</tr>
</tbody>
</table>

## Time Frame

- 1 Hour
- 24 Hours
- 7 Days
- 30 Days
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