Attacking VoIP

the attacks & the attackers

Obligatory whois

- Sandro Gauci (from .mt)
- Security researcher and Pentester
- SIPVicious / VOIPPACK for CANVAS
- VOIPSCANNER.com
- Not just about VoIP
- EnableSecurity

Agenda

- Get the basics out of the way
- How does SIP scanning work?
  - any advances in the area?
- What happens when you scan the ‘net
- Who is scanning the ‘net?
- ... why?

A primer on SIP

- Text based just like HTTP
- Mostly UDP port 5060
- Endpoints
- “Servers”
  - registrars
  - proxies

A primer on SIP

- Methods
  - INVITE gets things to buzz and ring
  - REGISTER sends phone calls your way
  - OPTIONS gives you supported options

method

request URI
sip address

Header

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <bob@biloxi.com>
From: Alice <alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 147
```

dest address

caller address

Body

```
v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 pc33.atlanta.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

media IP address

media rtp port

codecs

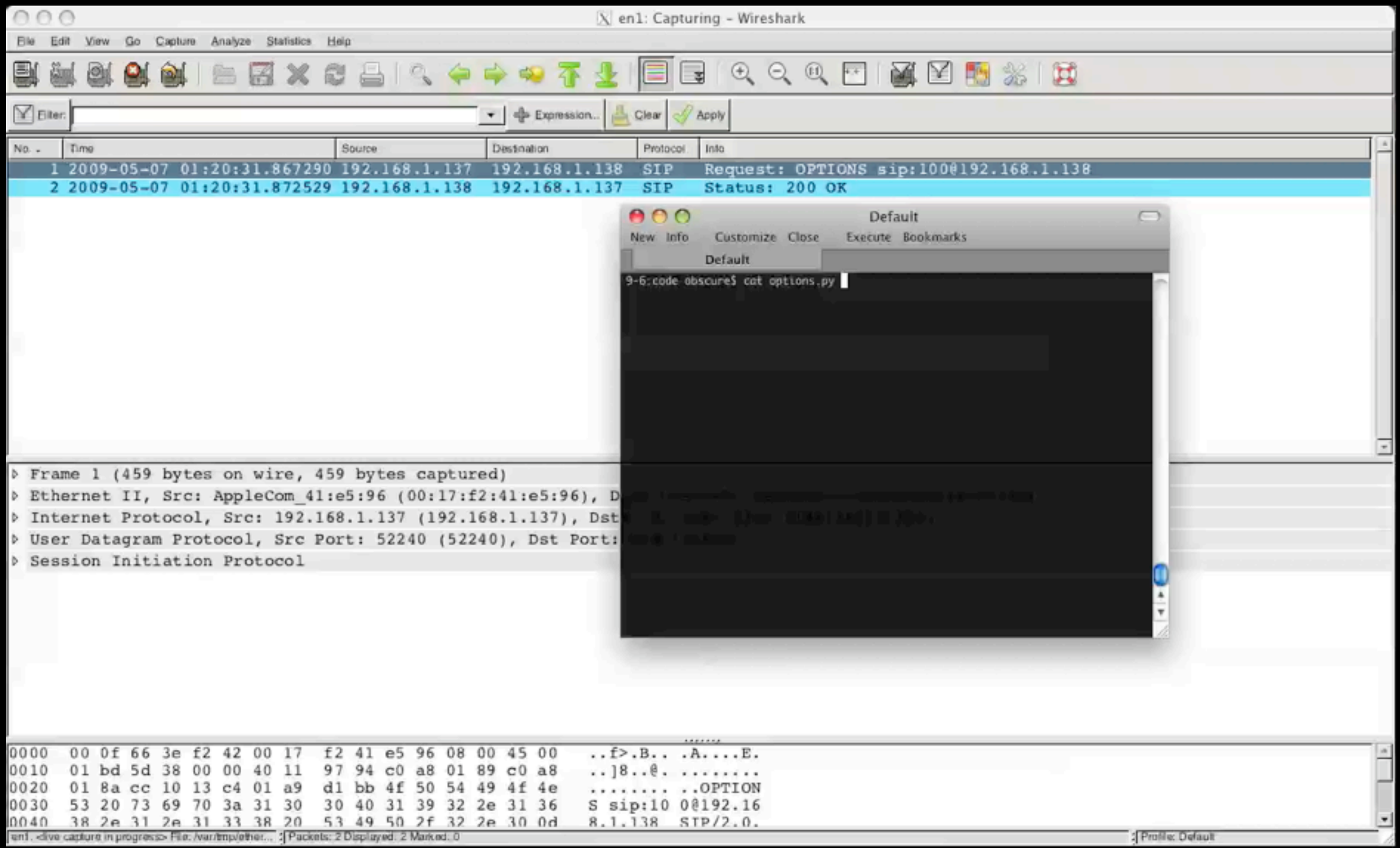
Scanning SIP

- Basic concept: elicit a response
- UDP has advantages for scanning
  - send and forget
  - no need to multiple sockets

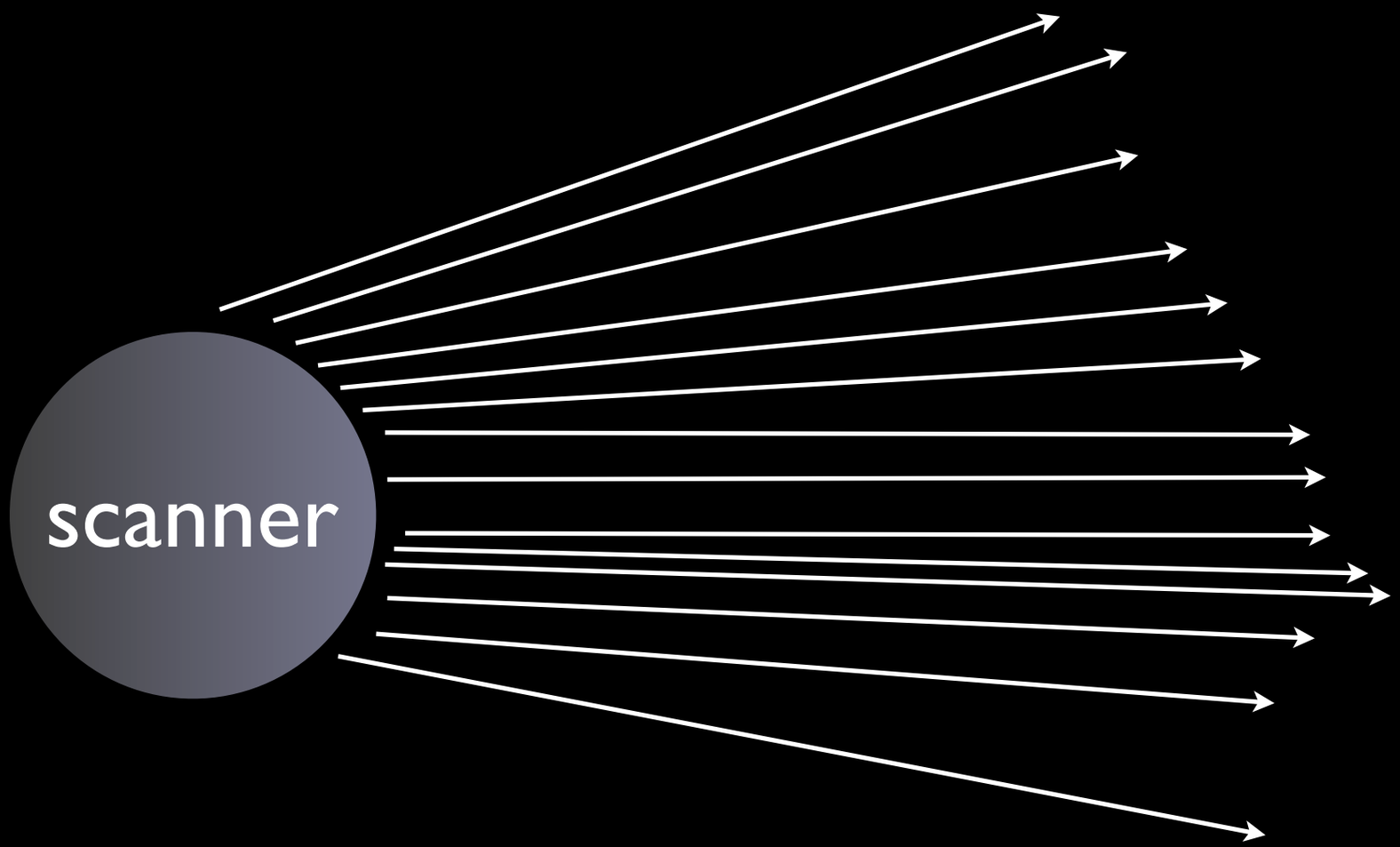
SIP: OPTIONS scan

SIP: OPTIONS scan

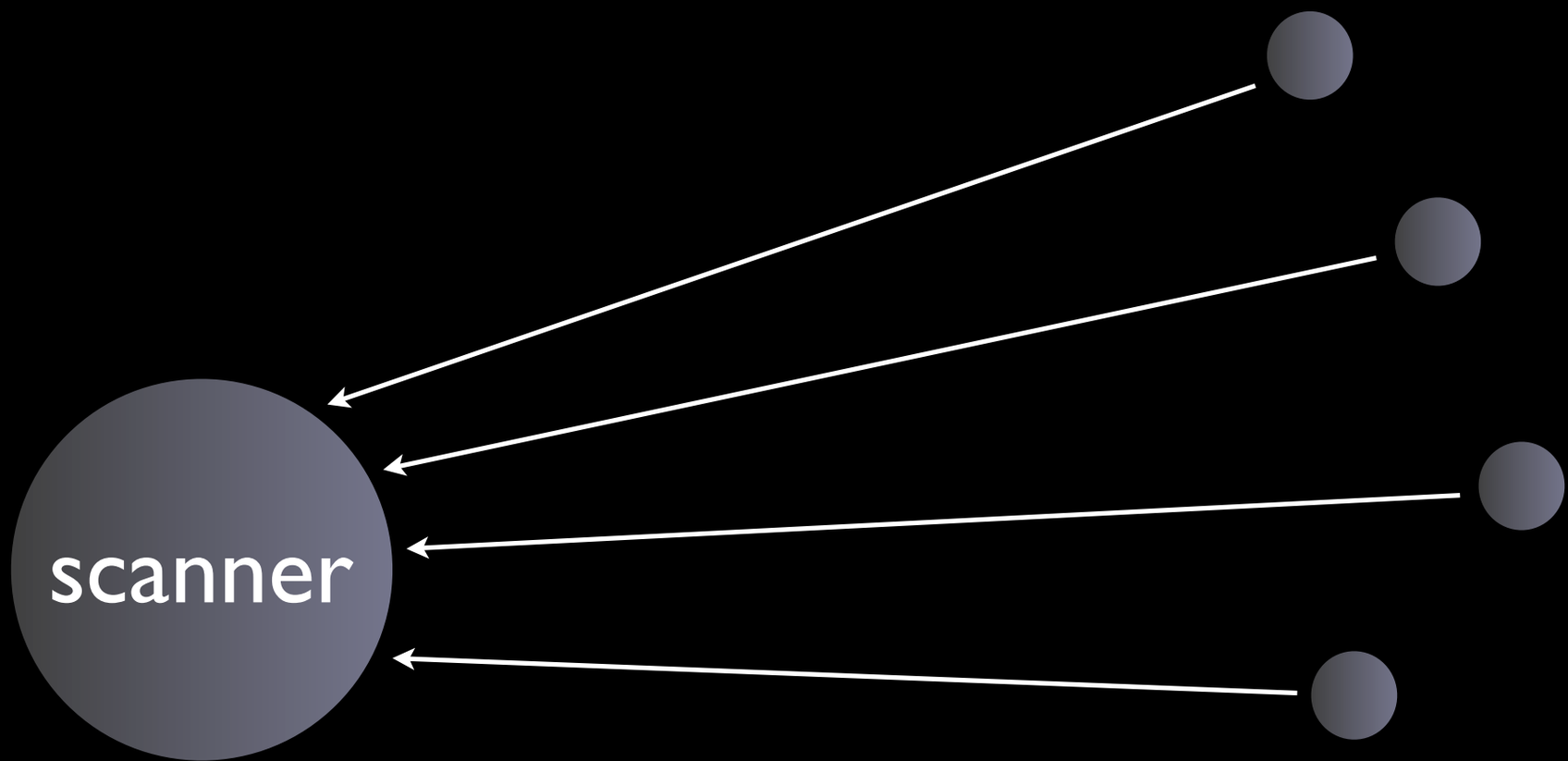
```
OPTIONS sip:2658@195.159.X.X SIP/2.0
Via: SIP/2.0/UDP 0.0.0.0:1498;branch=BCEA2F83-1CEF-FC6A-2989-54C18CE6425E;rport
Max-Forwards: 70
To: <sip:2658@195.159.X.X>
From: <sip:8571@195.159.X.X>;tag=723535DC-E71F-E3D4-D572-2B41E58782E8
Call-ID: 4203F1B5-3E1F-E6D6-32FF-B8C2DFAA190F
CSeq: 1 OPTIONS
Contact: <sip:@0.0.0.0:1498;>
Accept: application/sdp
Content-Length: 0
```


en1: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 2009-05-07 01:20:31.867290 192.168.1.137 192.168.1.138 SIP Request: OPTIONS sip:100@192.168.1.138
2 2009-05-07 01:20:31.872529 192.168.1.138 192.168.1.137 SIP Status: 200 OK
Default
New Info Customize Close Execute Bookmarks
Default
9-6:code obscure$ cat options.py
Frame 1 (459 bytes on wire, 459 bytes captured)
Ethernet II, Src: AppleCom_41:e5:96 (00:17:f2:41:e5:96), D
Internet Protocol, Src: 192.168.1.137 (192.168.1.137), Dst
User Datagram Protocol, Src Port: 52240 (52240), Dst Port:
Session Initiation Protocol
0000 00 0f 66 3e f2 42 00 17 f2 41 e5 96 08 00 45 00 ..f>.B.. .A....E.
0010 01 bd 5d 38 00 00 40 11 97 94 c0 a8 01 89 c0 a8 ..]8..@. ....
0020 01 8a cc 10 13 c4 01 a9 d1 bb 4f 50 54 49 4f 4e ....OPTION
0030 53 20 73 69 70 3a 31 30 30 40 31 39 32 2e 31 36 S sip:10 0@192.16
0040 38 2e 31 2e 31 33 38 20 53 49 50 2f 32 2e 30 0d 8.1.138 SIP/2.0.
en1: <live capture in progress> File: /var/tmp/ether...
Packets: 2 Displayed: 2 Marked: 0
Profile: Default

Scanning lots!



Scanning lots!



Scanning VoIP protocols

- SIP (various tools:
  mine are SIPVicious, VOIPPACK, voipscanner.com)
- IAX2 (VOIPPACK, iaxscan, enumIAX)
- Works in progress
  - SCCP
  - H.323
  - MGCP

Real life SIP scanning

- Different ranges
- Random scan
- Alternative ports
- Methods other than OPTIONS
- SRV records

Introducing svmap

- Trying out different ranges
  - 1.1.1.1-1.1.1.20
  - 1.1.1.1/24
  - 1.1.1-3.*

Introducing svmap

- Random scans
  - svmap.py --randomscan
  - svmap.py --randomize 1.1.1.*

Choose your target

- Can scan by IP address class
- Scan by provider
- Scanning whole countries is interesting
- Location based trends

Live demo showing svmap random scanning in action

```
-bash-3.1$
```

backup demo ;-)

Fingerprinting

- Sometimes the User-agent is not set
- Or modified (opensource SIP software)
- Solution: fingerprinting

Fingerprinting request vs response

- In a request, various things are generated "randomly"
  - From tag
  - Call-ID value
  - Branch value
- In a response, only the "To" tag is generated "randomly"

Headers of interest

```
SIP/2.0 404 Not found
Via: SIP/2.0/UDP 1.1.1.1:5061;branch=z9hG4bK-59472;received=1.1.1.1;rport=5061
From: "test" <sip:100@1.2.3.4:5060>;tag=d5a5bd3213c46cdd060c
To: "test" <sip:100@1.2.3.4:5060>;tag=as05610bff
Call-ID: 37012f88-24ac-44aa-ac45-2e6a05421e7d
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

Modified User-agent

```
SIP/2.0 404 Not found
Via: SIP/2.0/UDP 1.1.1.1:5061;branch=z9hG4bK-59472;received=1.1.1.1;rport=5061
From: "test" <sip:100@1.2.3.4:5060>;tag=d5a5bd3213c46cdd060c
To: "test" <sip:100@1.2.3.4:5060>;tag=as05610bff
Call-ID: 37012f88-24ac-44aa-ac45-2e6a05421e7d
CSeq: 1 REGISTER
User-Agent: MyVeryOwn PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

Give away

```
SIP/2.0 404 Not found
Via: SIP/2.0/UDP 1.1.1.1:5061;branch=z9hG4bK-59472;received=1.1.1.1;rport=5061
From: "test" <sip:100@1.2.3.4:5060>;tag=d5a5bd3213c46cdd060c
To: "test" <sip:100@1.2.3.4:5060>;tag=as05610bff
Call-ID: 37012f88-24ac-44aa-ac45-2e6a05421e7d
CSeq: 1 REGISTER
User-Agent: MyVeryOwn PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

Give away

```
SIP/2.0 404 Not found
Via: SIP/2.0/UDP 1.1.1.1:5061;branch=z9hG4bK-59472;received=1.1.1.1;rport=5061
From: "test" <sip:100@1.2.3.4:5060>;tag=d5a5bd3213c46cdd060c
To: "test" <sip:100@1.2.3.4:5060>;tag=as05610bff
Call-ID: 37012f88-24ac-44aa-ac45-2e6a05421e7d
CSeq: 1 REGISTER
User-Agent: MyVeryOwn PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

How is that generated?

```
snprintf(tagbuf, len, "as%08lx", ast_random());
```

Fingerprinting To Tag

Asterisk	as[0-9a-f]{8}
Sipura / Linksys SPA	[a-fA-F0-9]{16}i0
Cisco VoIP Gateway	[a-fA-F0-9]{6,8}-[a-fA-F0-9]{2,4}
AVM FRITZ!Box	[a-fA-F0-9]{16,29}

Order of headers

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 3.2.1.9:5061;branch=z9hG4bK-24832;rport;received=3.2.1.9
From: "hello" <sip:100@1.2.3.35:5060>;tag=d90a4f2313c4cc438e14
To: "hello" <sip:100@1.2.3.35:5060>;tag=as00ea0c68
Call-ID: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
CSeq: 1 OPTIONS
User-Agent: xxx voicemail
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Contact: <sip:1.2.3.35>
Accept: application/sdp
Content-Length: 0
```

Order of headers

```
SIP/2.0 404 Not Found
Via: SIP/2.0/UDP 3.2.1.9:5061;branch=z9hG4bK-59202;received=3.2.1.9;rport=5061
From: "hello" <sip:100@1.2.3.138:5060>;tag=d90a4f8a13c4d8bf89f5
To: "hello" <sip:100@1.2.3.138:5060>;tag=as263e3393
Call-ID: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
CSeq: 1 OPTIONS
User-Agent: xxx asterisk
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Accept: application/sdp
Content-Length: 0
```

Order of headers

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 3.2.1.9:5061;branch=z9hG4bK-2483
From: "hello" <sip:100@1.2.3.35:5060>;tag=d90a4f2
To: "hello" <sip:100@1.2.3.35:5060>;tag=as00ea0c6
Call-ID: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
CSeq: 1 OPTIONS
User-Agent: sipgate voicemail
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, S
Contact: <sip:1.2.3.35>
Accept: application/sdp
Content-Length: 0
```

```
SIP/2.0 404 Not Found
Via: SIP/2.0/UDP 3.2.1.9:5061;branch=z9hG4bK-
From: "hello" <sip:100@1.2.3.138:5060>;tag=d9
To: "hello" <sip:100@1.2.3.138:5060>;tag=as26
Call-ID: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
CSeq: 1 OPTIONS
User-Agent: sipbox asterisk
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REF
Supported: replaces
Accept: application/sdp
Content-Length: 0
```

Order of headers

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 3.2.1.9:5061;branch=z9hG4bK-2483
From: "hello" <sip:100@1.2.3.35:5060>;tag=d90a4f2
To: "hello" <sip:100@1.2.3.35:5060>;tag=as00ea0c6
Call-ID: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
CSeq: 1 OPTIONS
User-Agent: sipgate voicemail
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, S
Contact: <sip:1.2.3.35>
Accept: application/sdp
Content-Length: 0
```

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 3.2.1.9:5061;bra=z9hG4bK-
From: "hello" <sip:100@1.2.3.40:5060>;tag=d90
To: "hello" <sip:100@1.2.3.40:5060>;tag=cfbe3
Cseq: 1 REGISTER
Call-id: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
WWW-Authenticate: Digest realm="sipgate.at",
Content-Length: 0
```

Case for header names

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 3.2.1.9:5061;branch=z9hG4bK-2483
From: "hello" <sip:100@1.2.3.35:5060>;tag=d90a4f2
To: "hello" <sip:100@1.2.3.35:5060>;tag=as00ea0c6
Call-ID: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
CSeq: 1 OPTIONS
User-Agent: sipgate voicemail
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, S
Contact: <sip:1.2.3.35>
Accept: application/sdp
Content-Length: 0
```

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 3.2.1.9:5061;branch=z9hG4bK-
From: "hello" <sip:100@1.2.3.40:5060>;tag=d90
To: "hello" <sip:100@1.2.3.40:5060>;tag=cfbe3
Cseq: 1 REGISTER
Call-id: 6a53b3b9-3c0b-47d3-9e7f-b024ffe74663
WWW-Authenticate: Digest realm="sipgate.at",
Content-Length: 0
```

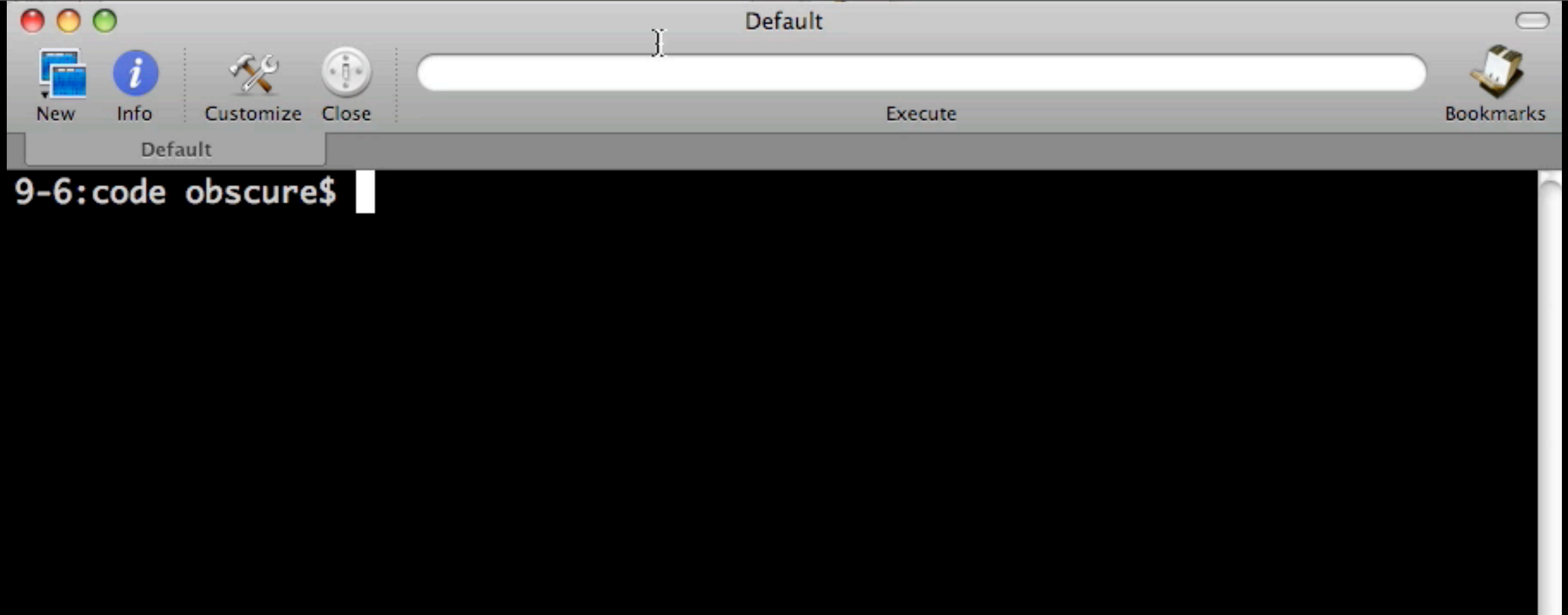
Fingerprinting SIP

- Just one packet needed
- To tag
- Headers
- Rewriting in progress

What else?

- Find out which extensions are on the PBX
- Break their password
- Try to relay a phone call (INVITE scan)
- Or just go ahead and own the PBX

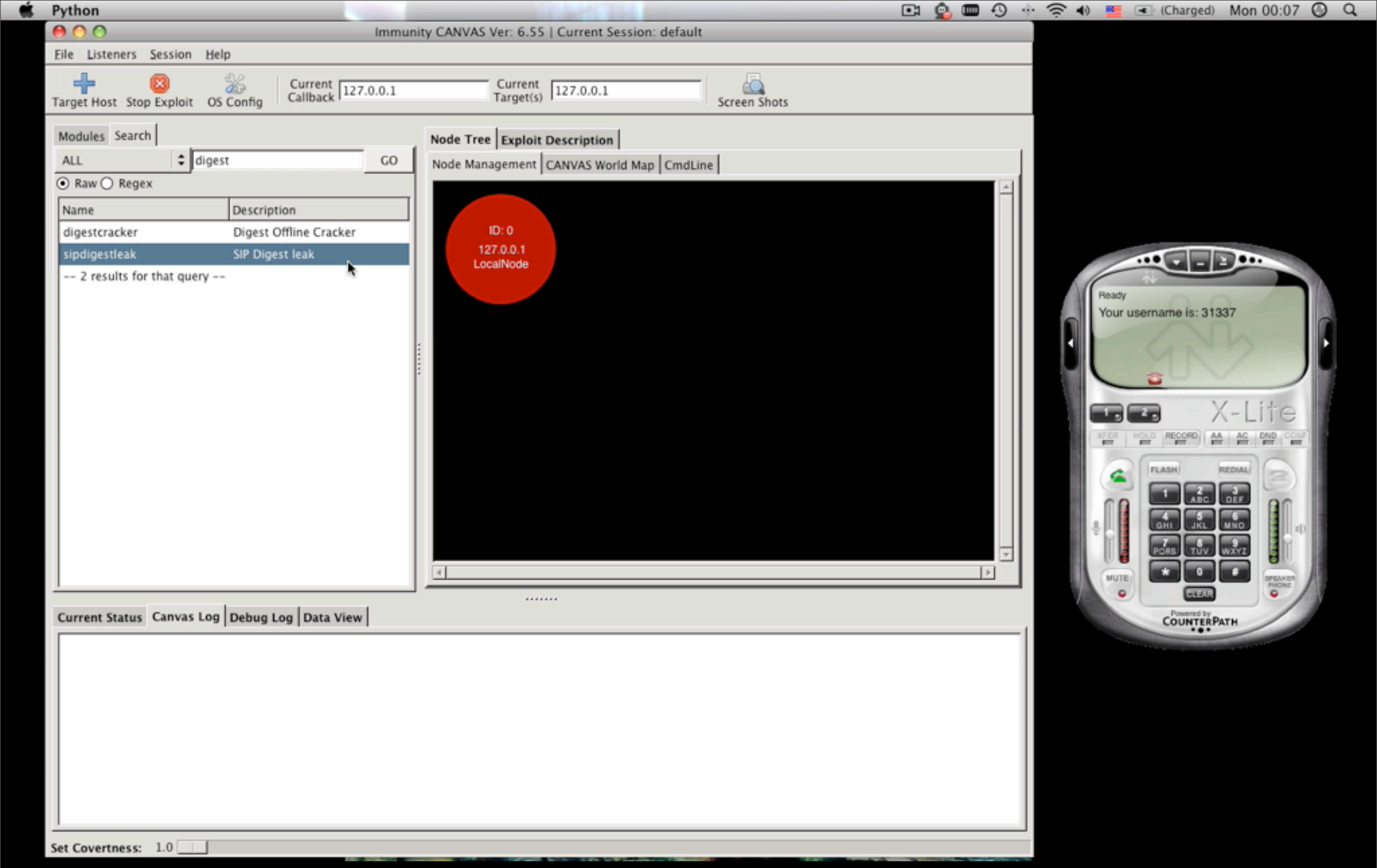
Demo showing how enumeration of extensions works


Default
New
Info
Customize
Close
Execute
Bookmarks
Default
9-6:code obscure$

svwar.py (SIPVicious) and sipenumerate (VOIPPACK) automate this fully

```
9-10:sipvicious obscure$
```

Demo showing SIP Digest Leak in action


Python
(Charged)
Mon 00:07
Immunity CANVAS Ver: 6.55 | Current Session: default
File
Listeners
Session
Help
Target Host
Stop Exploit
OS Config
Current Callback
127.0.0.1
Current Target(s)
127.0.0.1
Screen Shots
Modules
Search
ALL
digest
GO
Raw
Regex
Name
Description
digestcracker
Digest Offline Cracker
sipdigestleak
SIP Digest leak
-- 2 results for that query --
Node Tree
Exploit Description
Node Management
CANVAS World Map
CmdLine
ID: 0
127.0.0.1
LocalNode
Ready
Your username is: 31337
X-Lite
Powered by
COUNTERPATH
Current Status
Canvas Log
Debug Log
Data View
Set Covertness:
1.0

Demo showing Elastix 1.5.2 with exploitable VTiger

Chrome File Edit View History Bookmarks Window Help (Charged) Wed 21:34

Elastix - Login page

https://192.168.2.102/vtigercrm/

elastix
CUSTOM MADE TELEPHONY

» Welcome to Elastix

Please enter your username and password

Username:

Password:

Submit

Copyright © 2006 by PaloSanto Solutions

Waiting for 192.168.2.102...

INVITE scans

- INVITE gets thing to ring
- Many times it requires a valid sip uri
- The problem is ...

Some phones will ring on any number

Some misconfigured SIP gateways / servers will try to terminate the call

Analysis of a VoIP Attack

Klaus Darilion, IPCom GmbH, klaus.darilion@ipcom.at

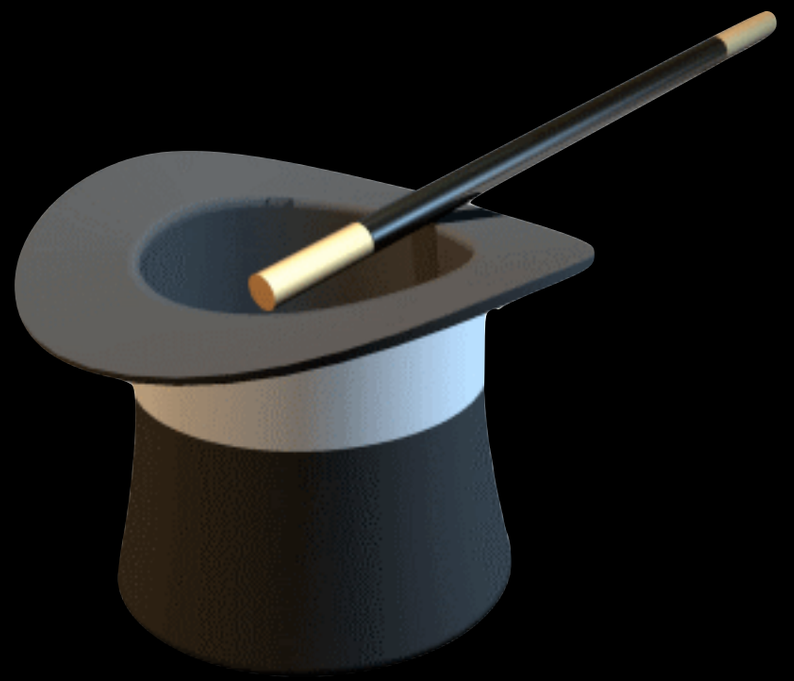
Abstract: Recently, several IT news websites reported VoIP attacks against home users, containing lots of myths and incorrect statements. Unfortunately, they also give wrong security advices. This article analyzes the attacks and describes the motivations behind. Further, it shows simple workarounds how "insecure" software can be used in a secure way.

```
02:12:42 SIP_TR> [GW] < Stack: from 213.130.74.70:3808
INVITE sip:8105255516900000@1.2.3.4;transport=udp SIP/2.0
Via: SIP/2.0/UDP 213.130.74.70:3808;branch=10010010110101111110111
00100213.130.74.701.2.3.41863480914;rport
Max-Forwards: 100
From: <sip:5199362832664@1.2.3.4>;tag=21671132663-
 49852691621671132663216711326631 3.130.74.70
To: <sip:8105255516900000@1.2.3.4>
Call-ID: 837648111000111011100100101101011011001110010010111
 0101111110111000100213.130.74.701.2.3.41863480914f
 df2388105255516900002167113266 3-
 450975916216711326632167113266 3213.130.74.70174046 6380
CSeq: 1 INVITE
Contact: <sip:fdf238@213.130.74.70:3808;transport=udp>
Content-Type: application/sdp
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK,
 REFER, REGISTER, SUBSCRIBE, UPDATE, PUBLISH
User-Agent: X-Lite release 1006e stamp 34025
Content-Length: 394
```

Introducing voiphun

- Short for “voip honeypot” :-)
- A very simple fake SIP registration server
- And fake proxy too (i.e. takes calls)
- Which can be used as a honeypot
- Still limited in functionality

What's in voiphun's hat?



```
INVITE sip:34911871524@1.2.3.4 SIP/2.0
Via: SIP/2.0/UDP 93.190.143.10:5060;branch=z9hG4bK1e5f004e;rport
Max-Forwards: 70
From: "MeucciSolutions" <sip:MeucciSolutions@93.190.143.10>;tag=as2e634a50
To: <sip:34911871524@1.2.3.4>
Contact: <sip:MeucciSolutions@93.190.143.10>
Call-ID: 5695a0171916fd5e353bdef71d0f1336@93.190.143.10
CSeq: 102 INVITE
User-Agent: MeucciSolutions
Date: Sun, 10 May 2009 15:39:15 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces, timer
Content-Type: application/sdp
Content-Length: 289

v=0
o=root 2093936706 2093936706 IN IP4 93.190.143.10
s=Asterisk PBX 1.6.0.5
c=IN IP4 93.190.143.10
t=0 0
m=audio 13280 RTP/AVP 8 0 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
a=ptime:20
a=sendrecv
```

```
INVITE sip:3619990127@1.2.3.4 SIP/2.0
Via: SIP/2.0/UDP 93.190.143.10:5060;branch=z9hG4bK553a8ca4;rport
Max-Forwards: 70
From: "MeucciSolutions" <sip:MeucciSolutions@93.190.143.10>;tag=as059768a7
To: <sip:3619990127@1.2.3.4>
Contact: <sip:MeucciSolutions@93.190.143.10>
Call-ID: 4700633d2a3c0a34327ce2e07668ea23@93.190.143.10
CSeq: 102 INVITE
User-Agent: MeucciSolutions
Date: Sun, 10 May 2009 16:08:05 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces, timer
Content-Type: application/sdp
Content-Length: 289

v=0
o=root 2093113969 2093113969 IN IP4 93.190.143.10
s=Asterisk PBX 1.6.0.5
c=IN IP4 93.190.143.10
t=0 0
m=audio 16362 RTP/AVP 8 0 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
a=ptime:20
a=sendrecv
```

```
INVITE sip:00349118715 24@1.2.3.4 SIP/2.0
Via: SIP/2.0/UDP 93.190.143.10:5060;branch=z9hG4bK63f6e79c;rport
Max-Forwards: 70
From: "MeucciSolutions" <sip:MeucciSolutions@93.190.143.10>;tag=as5b7d22e8
To: <sip:00349118715 24@1.2.3.4>
Contact: <sip:MeucciSolutions@93.190.143.10>
Call-ID: 1d6c23fc3cb12618507211d8597aad10@93.190.143.10
CSeq: 102 INVITE
User-Agent: MeucciSolutions
Date: Sun, 10 May 2009 18:42:34 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces, timer
Content-Type: application/sdp
Content-Length: 289

v=0
o=root 1890643109 1890643109 IN IP4 93.190.143.10
s=Asterisk PBX 1.6.0.5
c=IN IP4 93.190.143.10
t=0 0
m=audio 18572 RTP/AVP 8 0 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
a=ptime:20
a=sendrecv
```

Who are Meucci Solutions anyway?

meucci solutions

SEARCH

Home - Contact - Partners - Access plan

About us | Solutions | Careers | News & Events

Home > Complaints

COMPLAINTS

Dear visitor,

Recently we have been receiving complaints about nuisance calls allegedly made in our name. We would like to apologize for the inconvenience this causes you.

After thorough investigation we can assure you that Meucci Solutions has not made these calls. A third party trying to harm our company is maliciously spoofing our company name in the Caller-ID field.

To be able to trace the perpetrators and take action, we need your collaboration.

Therefore we are asking you to send the following details to complaints@meucci-solutions.com:

- The telephone or switchboard number that received the calls
- Date and time of the calls received
- Caller ID information (what you saw on the screen)
- Duration of the calls
- The name of your telephone operator or service-provider

We would like to thank you for your understanding and collaboration.

Basic free calling

- Someone actually configured a softphone to use my honeypot
- Not a scanner ..

```
REGISTER sip:xx.xx.xx.xx; SIP/2.0
Via: SIP/2.0/UDP 188.27.208.189:62399;branch=z9hG4bK-d8754z-d97d7324ef9fe3b9-1---
d8754z-
Max-Forwards: 70
Contact: <sip:100@188.27.208.189:62399;rinstance=27d34fb7751fabd2;>
To: "UNKNOWN"<sip:>
From: "UNKNOWN"<sip:>;tag=3832fc23
Call-ID: OWE4NjIyODhhMjgxOGQ5OGRiNWFlYmEyMmNiYmJjZjQ.
CSeq: 1 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
User-Agent: Zoiper rev.5324
Allow-Events: presence
Content-Length: 0
```

```
INVITE sip:00423662701946@xx.xx.xx.xx;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 188.27.208.189:62399;branch=z9hG4bK-d8754z-ffab3c4b5a504640-1---
d8754z-
Max-Forwards: 70
Contact: <sip:100@188.27.208.189:62399;transport=UDP>
To: <sip:00423662701946@xx.xx.xx.xx;transport=UDP>
From: "UNKNOWN"<sip:100@xx.xx.xx.xx;transport=UDP>;tag=9a46293c
Call-ID: OGVmNmI1NmU3MTVmYTBmMTliMWZjMzdlYjI2N2U3ZTk.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
Content-Type: application/sdp
User-Agent: Zoiper rev.5324
Content-Length: 332

v=0
o=Zoiper_user 0 0 IN IP4 188.27.208.189
s=Zoiper_session
c=IN IP4 188.27.208.189
t=0 0
m=audio 65287 RTP/AVP 3 0 8 110 98 101
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:110 speex/8000
a=rtpmap:98 iLBC/8000
a=fmtp:98 mode=30
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

```
INVITE sip:0037091009112@xx.xx.xx.xx;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 188.27.208.189:62399;branch=z9hG4bK-d8754z-025d9d26e0a72a55-1---
d8754z-
Max-Forwards: 70
Contact: <sip:100@188.27.208.189:62399;transport=UDP>
To: <sip:0037091009112@xx.xx.xx.xx;transport=UDP>
From: "UNKNOWN"<sip:100@xx.xx.xx.xx;transport=UDP>;tag=92432566
Call-ID: MTcxMzViODI1NmU5ZDRhYTA1ODRkNDUzZGVhODRhZWE.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
Content-Type: application/sdp
User-Agent: Zoiper rev.5324
Content-Length: 332

v=0
o=Zoiper_user 0 0 IN IP4 188.27.208.189
s=Zoiper_session
c=IN IP4 188.27.208.189
t=0 0
m=audio 65287 RTP/AVP 3 0 8 110 98 101
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:110 speex/8000
a=rtpmap:98 iLBC/8000
a=fmtp:98 mode=30
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

```
INVITE sip:002437701248@xx.xx.xx.xx;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 188.27.208.189:62399;branch=z9hG4bK-d8754z-9452e55e784f770a-1---
d8754z-
Max-Forwards: 70
Contact: <sip:100@188.27.208.189:62399;transport=UDP>
To: <sip:002437701248@xx.xx.xx.xx;transport=UDP>
From: "UNKNOWN"<sip:100@xx.xx.xx.xx;transport=UDP>;tag=770afa6d
Call-ID: MzM1ZWRhNjhiZGQyMzI1ZGQzNjEzYmI2OGEyMzZlYTM.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
Content-Type: application/sdp
User-Agent: Zoiper rev.5324
Content-Length: 332

v=0
o=Zoiper_user 0 0 IN IP4 188.27.208.189
s=Zoiper_session
c=IN IP4 188.27.208.189
t=0 0
m=audio 65287 RTP/AVP 3 0 8 110 98 101
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:110 speex/8000
a=rtpmap:98 iLBC/8000
a=fmtp:98 mode=30
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

I <3 Patterns

- INVITE scans bruteforces phone numbers
- Why not extract those numbers?
- Group them by source IP / country

INVITE scan I

Came from Romania Data Systems network

```
00000447799584555
0000441372456539
000114420867023l5
000144012987090l
00044162262038l
0011447876617548
001442075828187
00441189780316
011442076339733
01447850294946
0442078375450
1442072425376
900441767677666
9011442082163104
90447973642015
9442074998161
```

INVITE scan 2

Also from China Telecom (Guangdong) network

```
#442076501050
00#442076501050
011#442076501050
011441616606065
0442076501050
442076501050
900442076501050
9011442076501050
9442076501050
```

fax number

INVITE scan 3

Came from China Telecom (Shanxi) network

```
00000447799584555
0000441372456539
000044207629734 7
00011442086702315
0001440129870903
0001441844208220
000441622620388
000442073878081
0011442076381111
0011447876617548
001442075828187
001447775742174
00441189780316
011442076339733
012441535610840
01447024074657
-- clipped --
```

INVITE scan 4

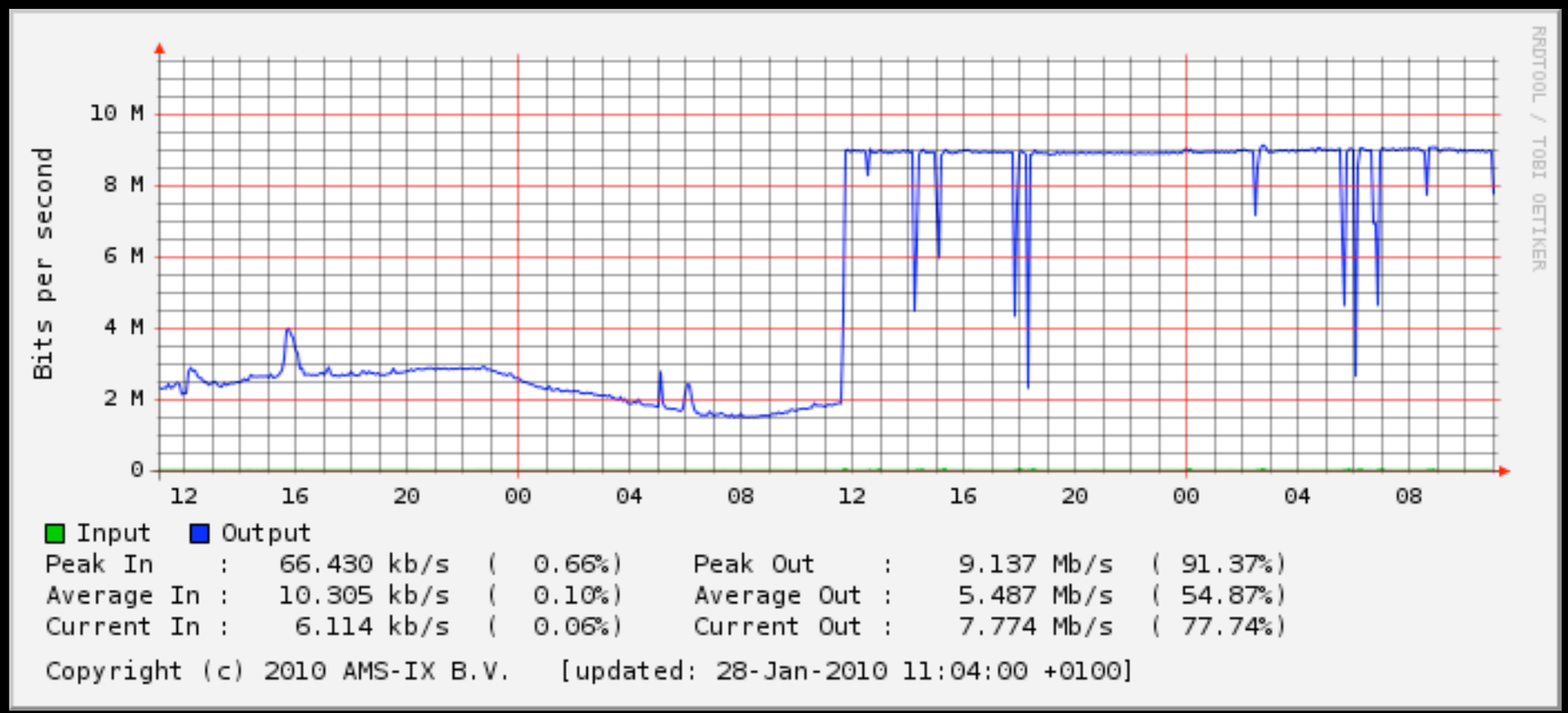
Came from ProXad network

```
33681368319
37322719718
33681368319
37322719718
33681368319
37322719718
33681368319
33681368319
```

The RIPE experiment

- 2010-01-27 they started announcing 1.1.1.0/24
- Only 10 MBit port
- It was maxed out immediately

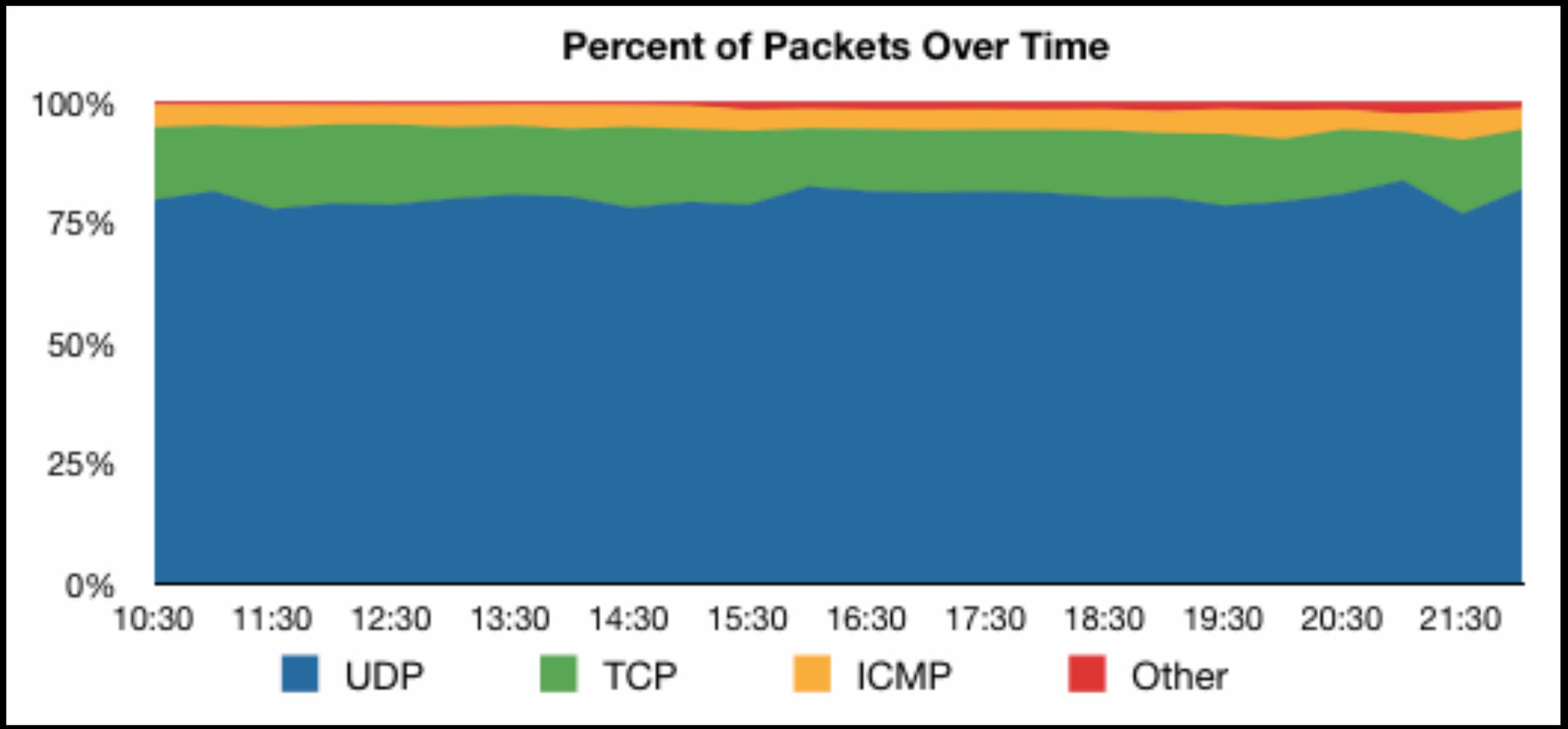
The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

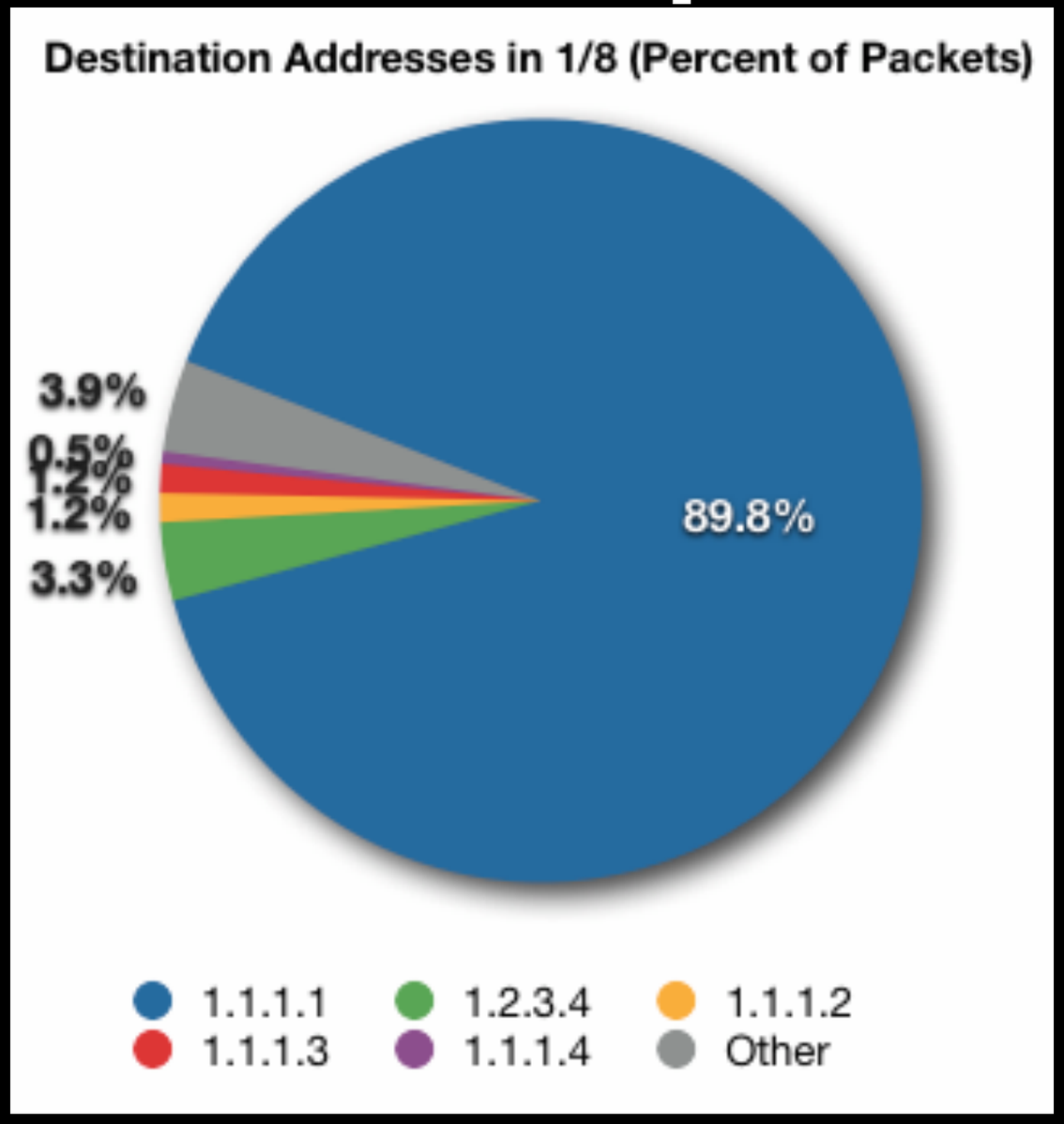
The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

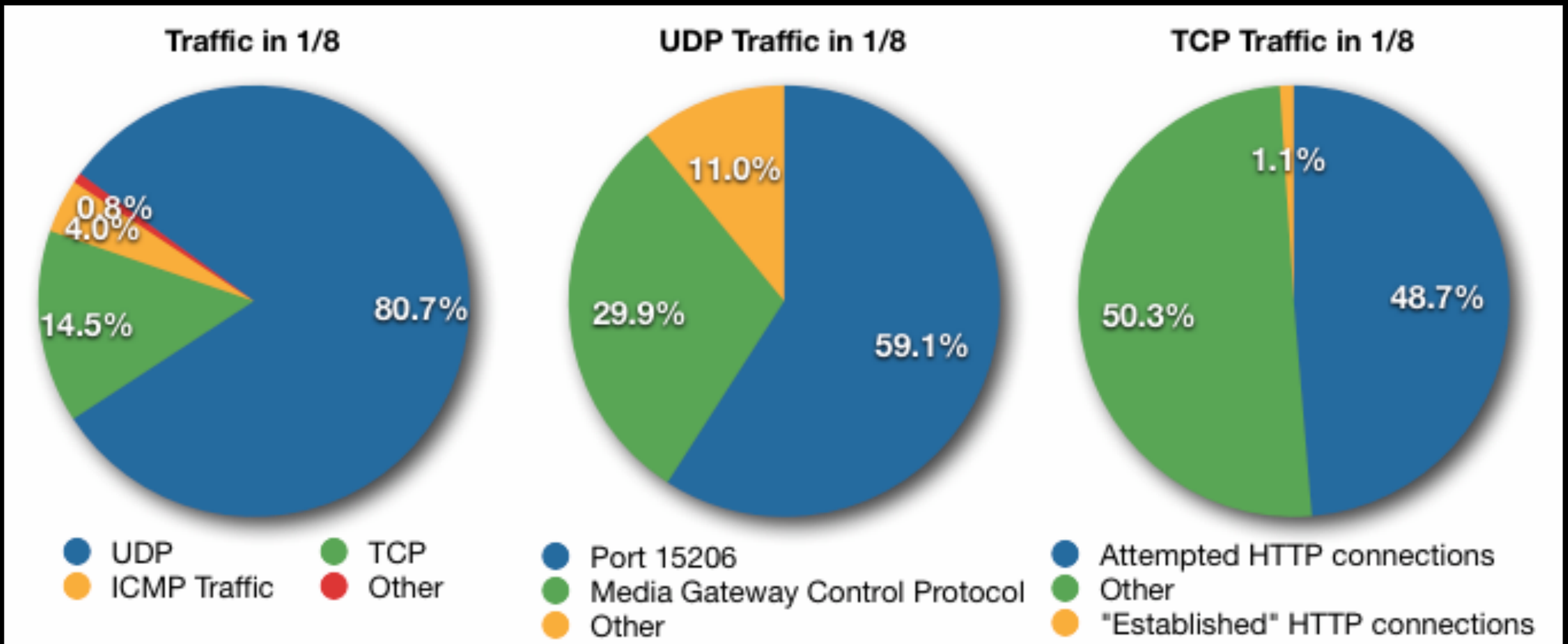
The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

The RIPE experiment



graph from RIPE blog

http://labs.ripe.net/content/pollution-18

The RIPE experiment

the part that i found interesting:

"We found that almost 60% of the UDP packets are sent towards the IP address 1.1.1.1 on port 15206 which makes up the largest amount of packets seen by our RRC. Most of these packets start their data section with 0x80, continue with seemingly random data and are padded to 172 bytes with an (again seemingly random) 2 byte value. Some sources (http://www.proxyblind.org/trojan.shtml) list the port as being used by a trojan called "KiLo", however information about it seem sparse."

quoting the RIPE blog

http://labs.ripe.net/content/pollution-18

back in voiphun land

```
INVITE sip:011442083327467@re.pl.ac.ed SIP/2.0
Via: SIP/2.0/UDP 83.142.202.195:3058;branch=ca4b60ae7ba821fREPLACEDjrgrg;rport
From: <sip:sip@83.142.202.195>;tag=Za4b60aeREPLACED
To: <sip:011442083327467@re.pl.ac.ed>
Contact: <sip:sip@83.142.202.195>
Call-ID: 213948958-00227506489-384748@83.142.202.195
CSeq: 102 INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Content-Type: application/sdp
Content-Length: 503

v=0
o=sip 2147483647 1 IN IP4 1.1.1.1
s=sip
c=IN IP4 1.1.1.1
t=0 0
m=audio 15206 RTP/AVP 10 4 3 0 8 112 5 7 18 111 101
a=rtpmap:10 L16/8000
a=rtpmap:4 G723/8000
a=fmtp:4 annexa=no
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:112 AAL2-G726-32/8000
a=rtpmap:5 DVI4/8000
a=rtpmap:7 LPC/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:111 G726-32/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
a=ptime:20
a=sendrecv
```

RTP Stream goes to IP 1.1.1.1

on port 15206

RTP & SDP

- RTP (almost) always starts with an 0x80
- If an INVITE is accepted the RTP stream is sent to the IP in the SDP
- Yet another reflected DDoS opportunity?

Profit?

- Phone fraud has been going on for a while
- Phone call termination cost money
- Premium numbers even more

One scheme

- Find SIP PBXs that have weak passwords
- Route phone calls through them
- Provide line termination to VoIP providers

Others

- May involve premium numbers
- Denial of Service can be a huge problem
- Millions of dollars in losses have been mentioned before (in toll fraud)

Thanks

- The Hackito Ergo Sum team
- Sn0rky, Sjur & others who helped
- SIPVicious contributors and users

More at..

- EnableSecurity.com/research
- Sipvicious.org
- VOIPSA.org

Q.A

alternatively contact me

sandro@enablesecurity.com