Simwood

VoIP Fraud Analysis

Simwood eSMS Limited
https://www.simwood.com/
@simwoodesms
Tel: 029 2120 2120

Simon Woodhead
Managing Director
simon.woodhead@simwood.com

INTRODUCTION

Wholesale Voice

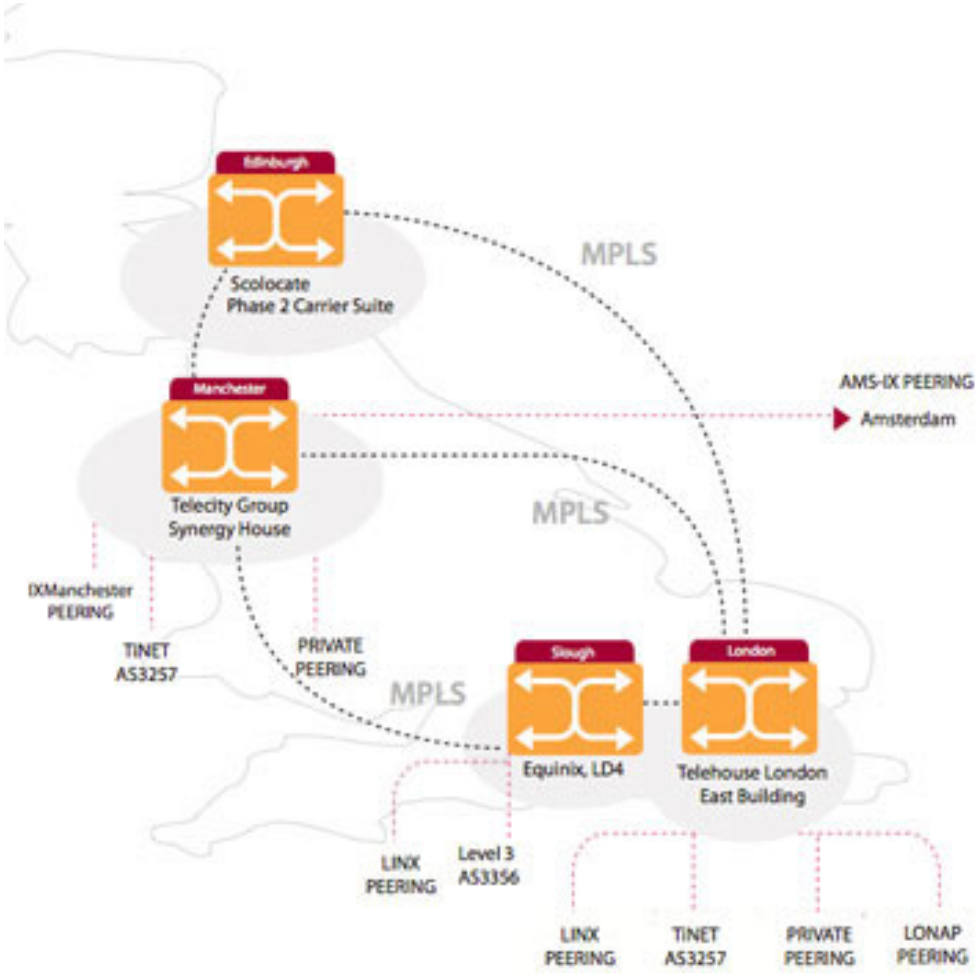
(and fax!)

UK Numbering

Termination

UK PSTN Virtual Interconnect

INTRODUCTION



INTRODUCTION

https://www.simwood.com

http://blog.simwood.com

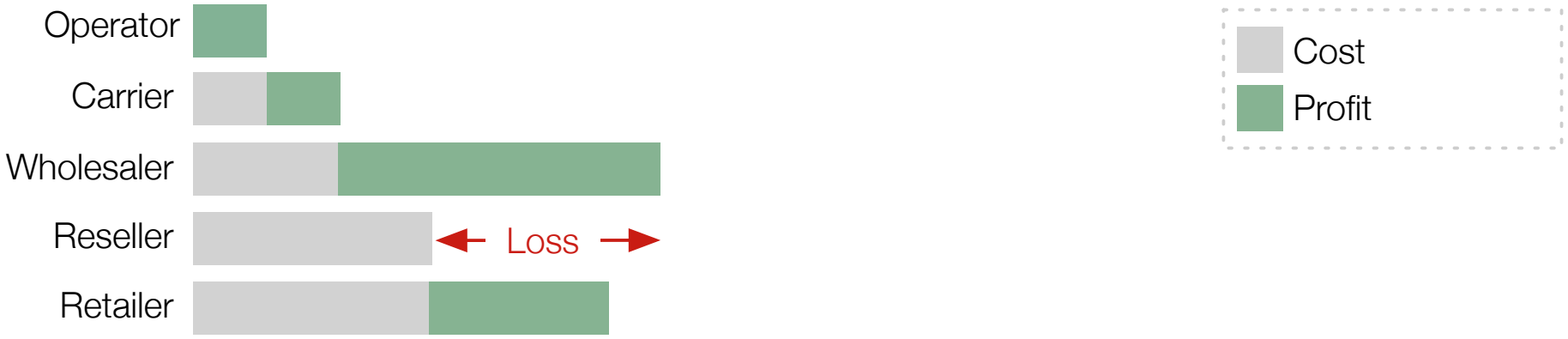
TOLL FRAUD & DIAL THROUGH FRAUD

$46bn

(but essentially unlimited)

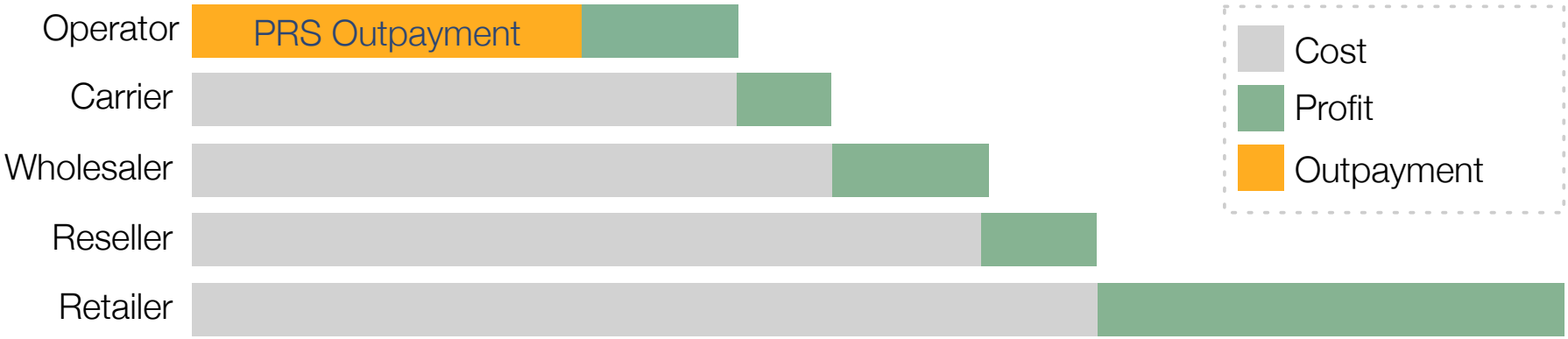
TOLL FRAUD & DIAL THROUGH FRAUD

TOLL FRAUD & DIAL THROUGH FRAUD

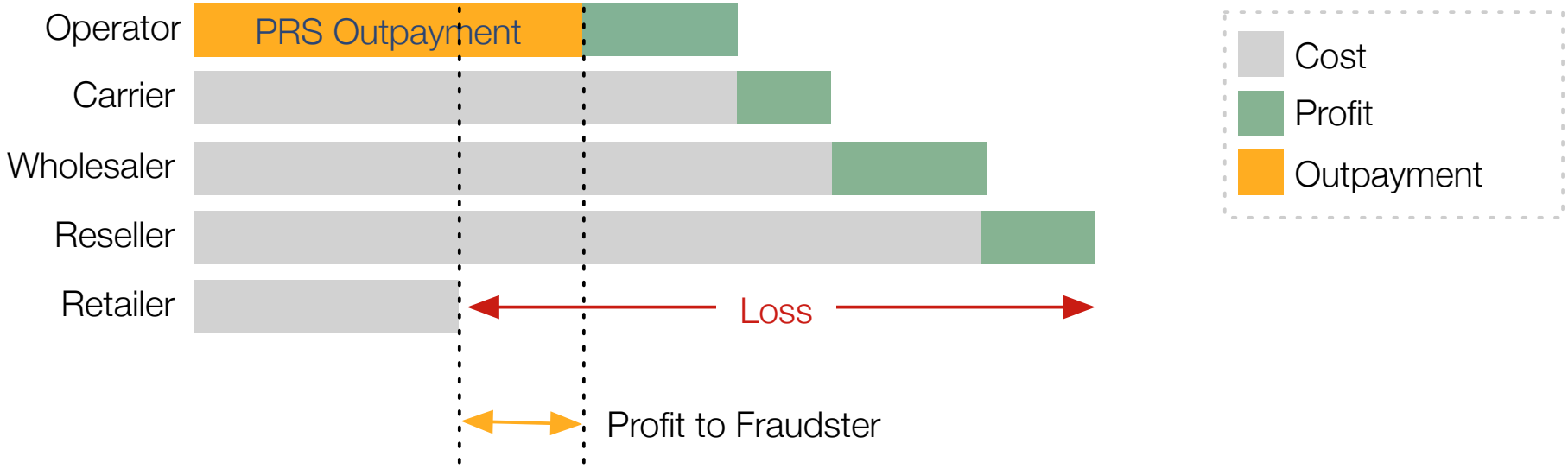


Simwood

TOLL FRAUD & DIAL THROUGH FRAUD



TOLL FRAUD & DIAL THROUGH FRAUD

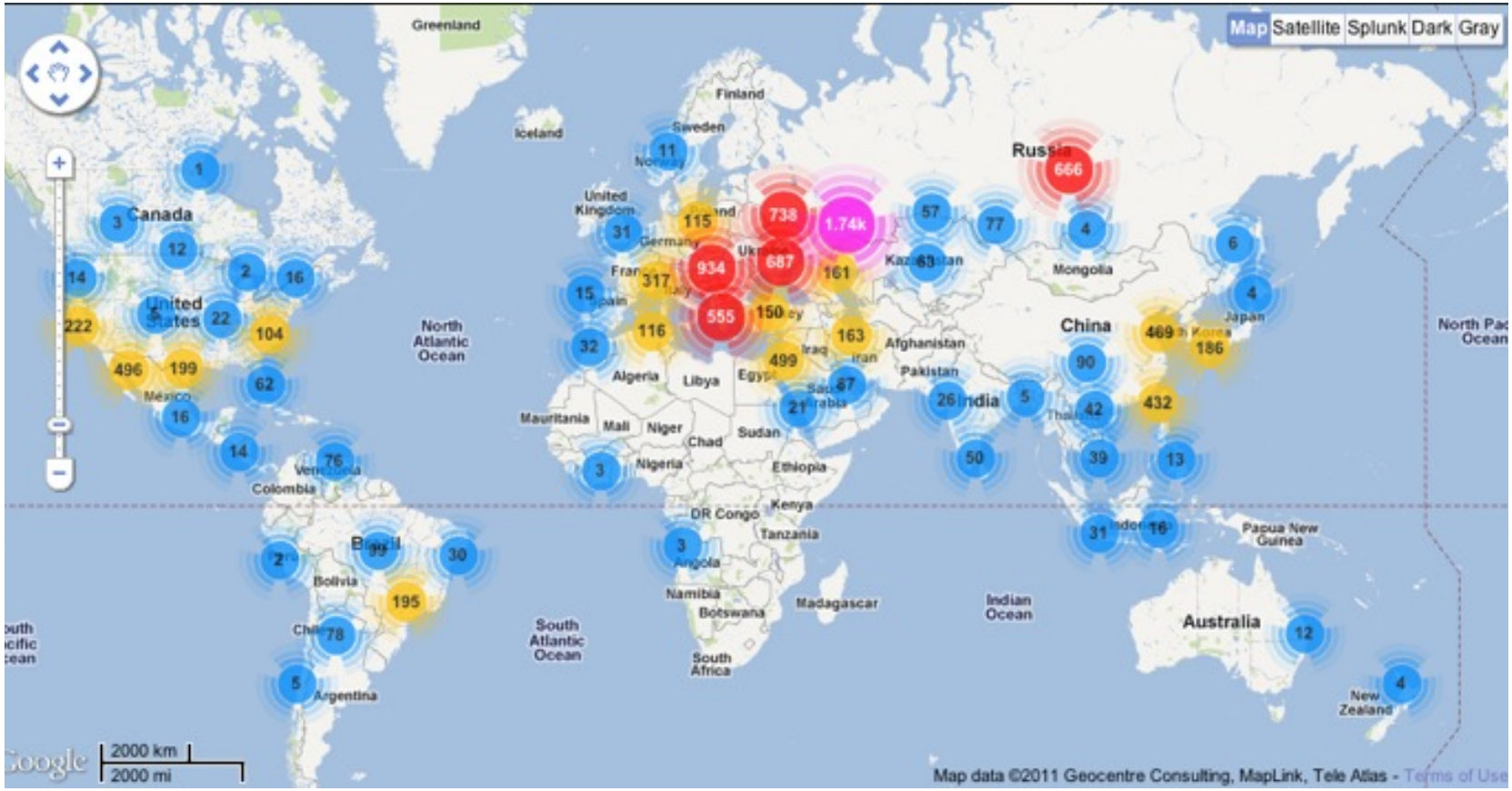


COMMERCIAL PRESSURE

VOICE IS BECOMING A FEATURE,
RATHER THAN A SERVICE

THE WISE MINIMISE RISK,
RATHER THAN MAXIMISE THEORETICAL MARGIN

SIMWOOD HONEYPOT



60 minutes in the Simwood Darknet on a Sunday afternoon

SIMWOOD HONEYPOT

http://mirror.simwood.com/honeypot

SIP Scan

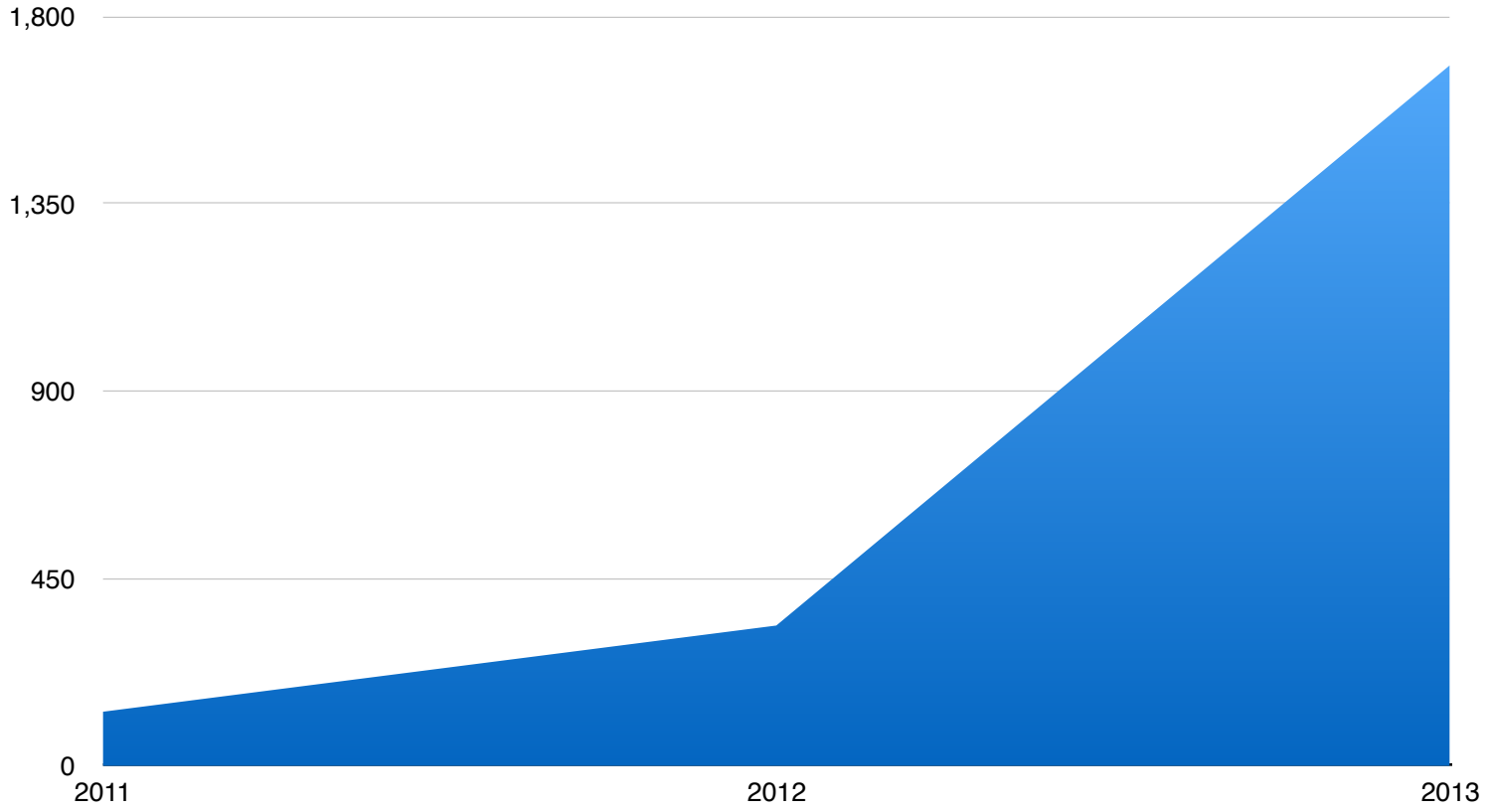
Stage 1: Reconnaissance

KEY INTRUSION METHODS
SIP SCAN

```
OPTIONS sip:100@XXX.XXX.XXX.XXX SIP/2.0
Via: SIP/2.0/UDP XXX.XXX.XXX.XXX:5151;branch=z9hG4bK-4181329969;rport
Content-Length: 0
From: "sipvicious"<sip:100@1.1.1.1>; tag=6332303064323361313363340132…
Accept: application/sdp
User-Agent: friendly-scanner
To: "sipvicious"<sip:100@1.1.1.1>
Contact: sip:100@XXX.XXX.XXX.XXX:5151
CSeq: 1 OPTIONS
```

KEY INTRUSION METHODS

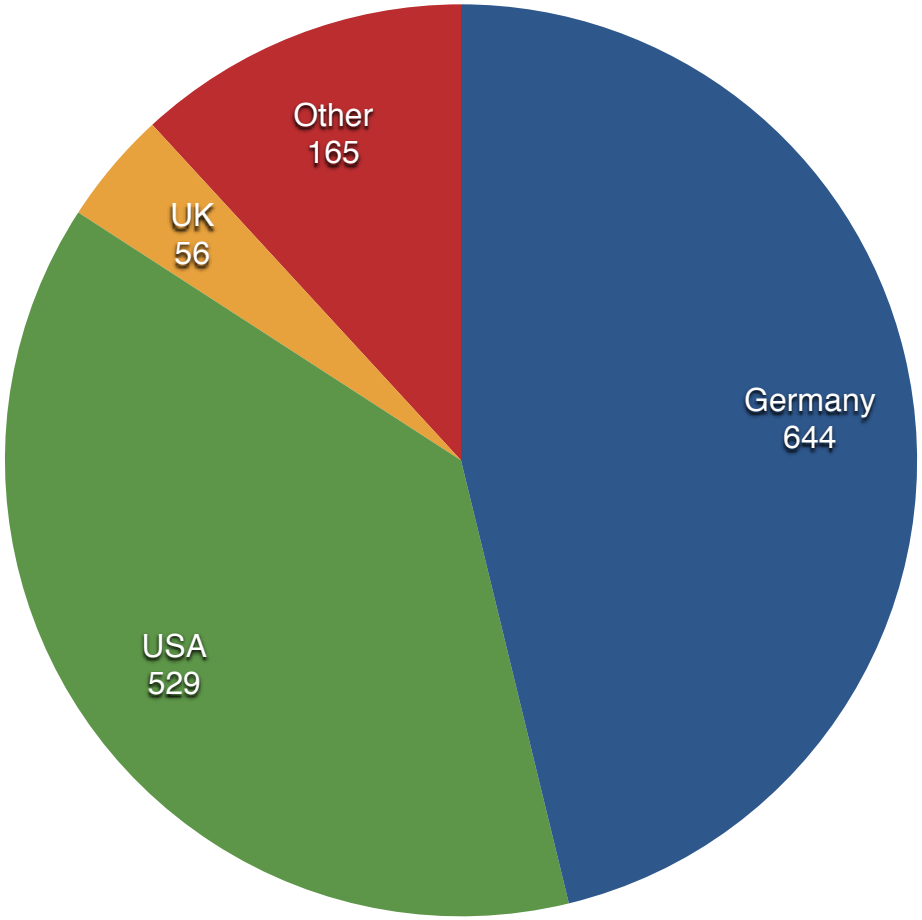
SIP SCAN



Growth in reconnaissance traffic (events by year)

KEY INTRUSION METHODS

SIP SCAN



Sources of reconnaissance traffic (12 months)

SIP Scan

Stage 2:
Scan

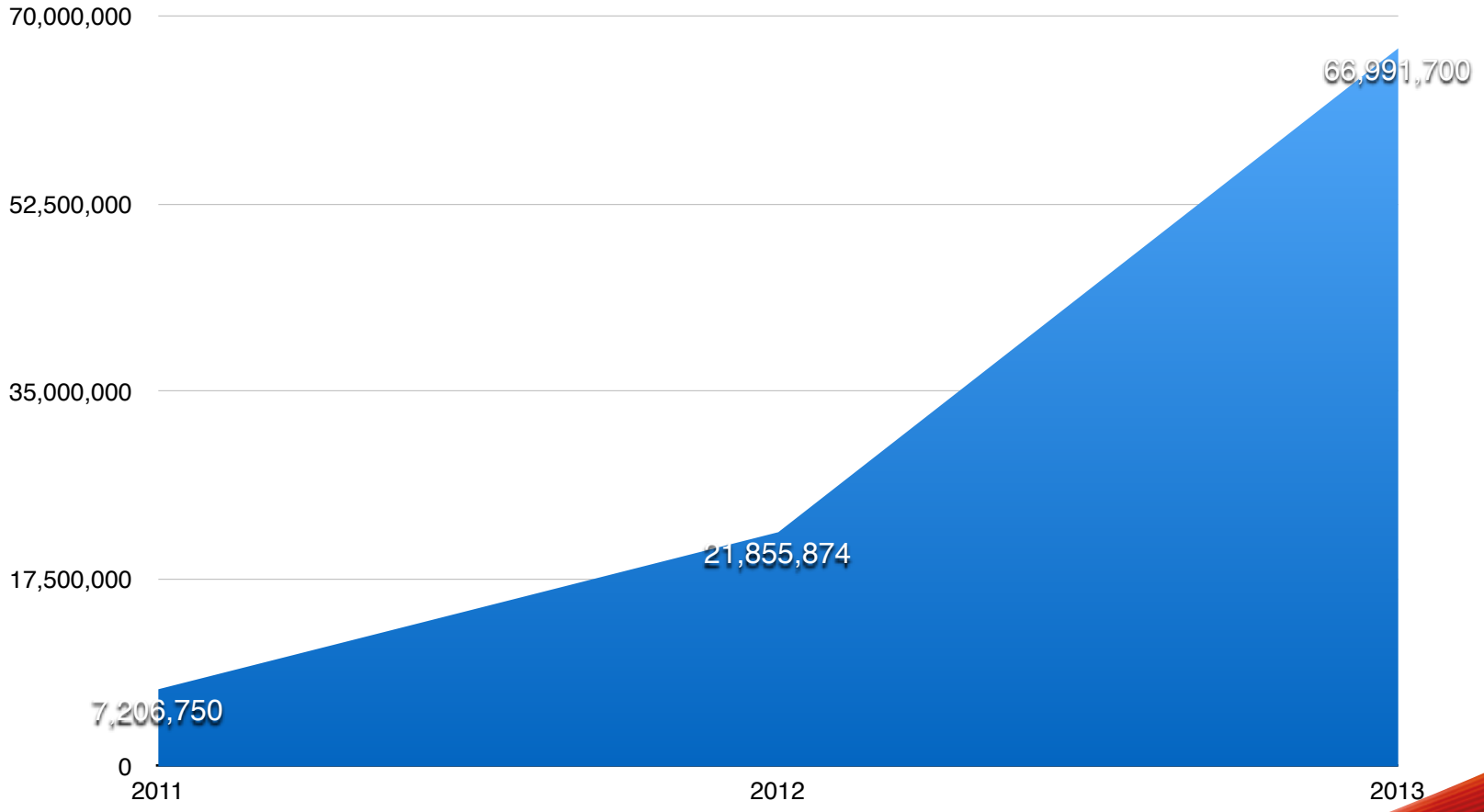
KEY INTRUSION METHODS
SIP SCAN

```
REGISTER sip:XXX.XXX.XXX.XXX SIP/2.0
To: <sip:1002@XXX.XXX.XXX.XXX>
From: <sip:1002@XXX.XXX.XXX.XXX>;tag=ba255b19
Via: SIP/2.0/UDP XXX.XXX.XXX.XXX:11184;branch=z9hG4bK-d87543-1477;rport
Call-ID: 8f60483ce717142b
CSeq: 1 REGISTER
Contact: <sip:1002@XXX.XXX.XXX.XXX:11184>
Expires: 3600
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, NOTIFY, MESSAGE, SUBSCRIBE…
User-Agent: eyeBeam release 3006o stamp 17551
Content-Length: 0
```

Simwood

KEY INTRUSION METHODS

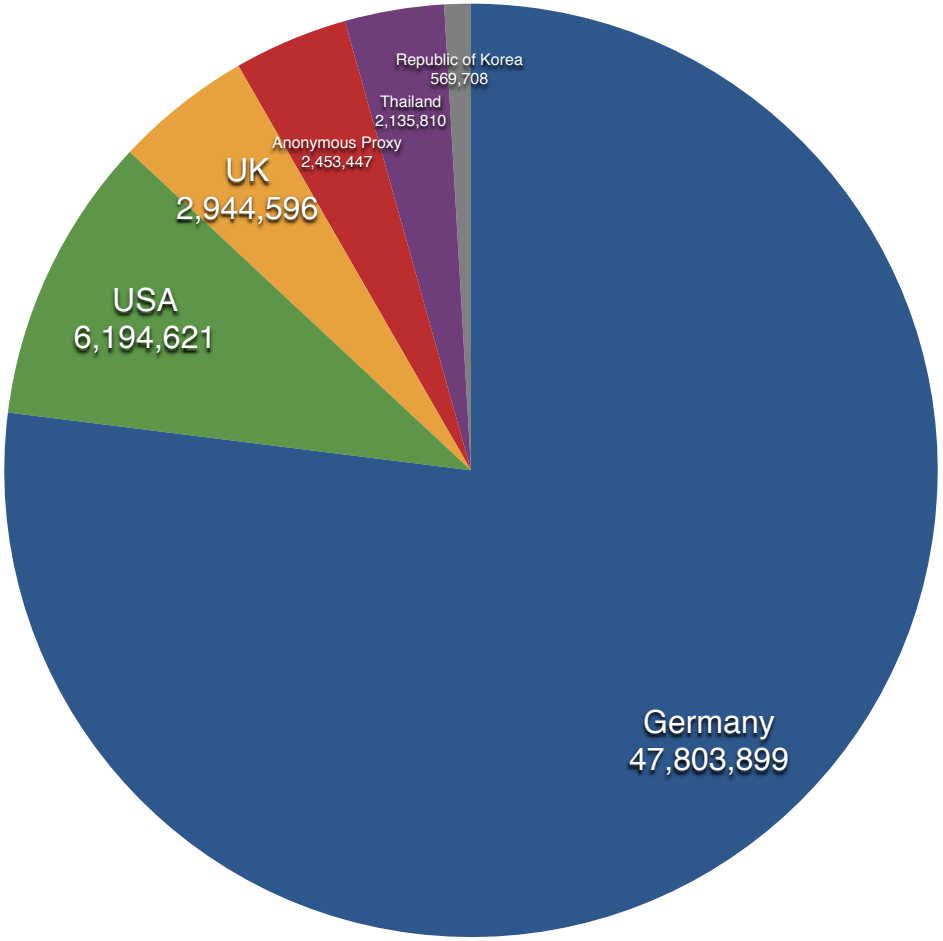
SIP SCAN



Growth in scan traffic (events by year)

KEY INTRUSION METHODS

SIP SCAN



Sources of scan traffic (12 months)

KEY INTRUSION METHODS

Targeted Exploit

Auto-provisioning

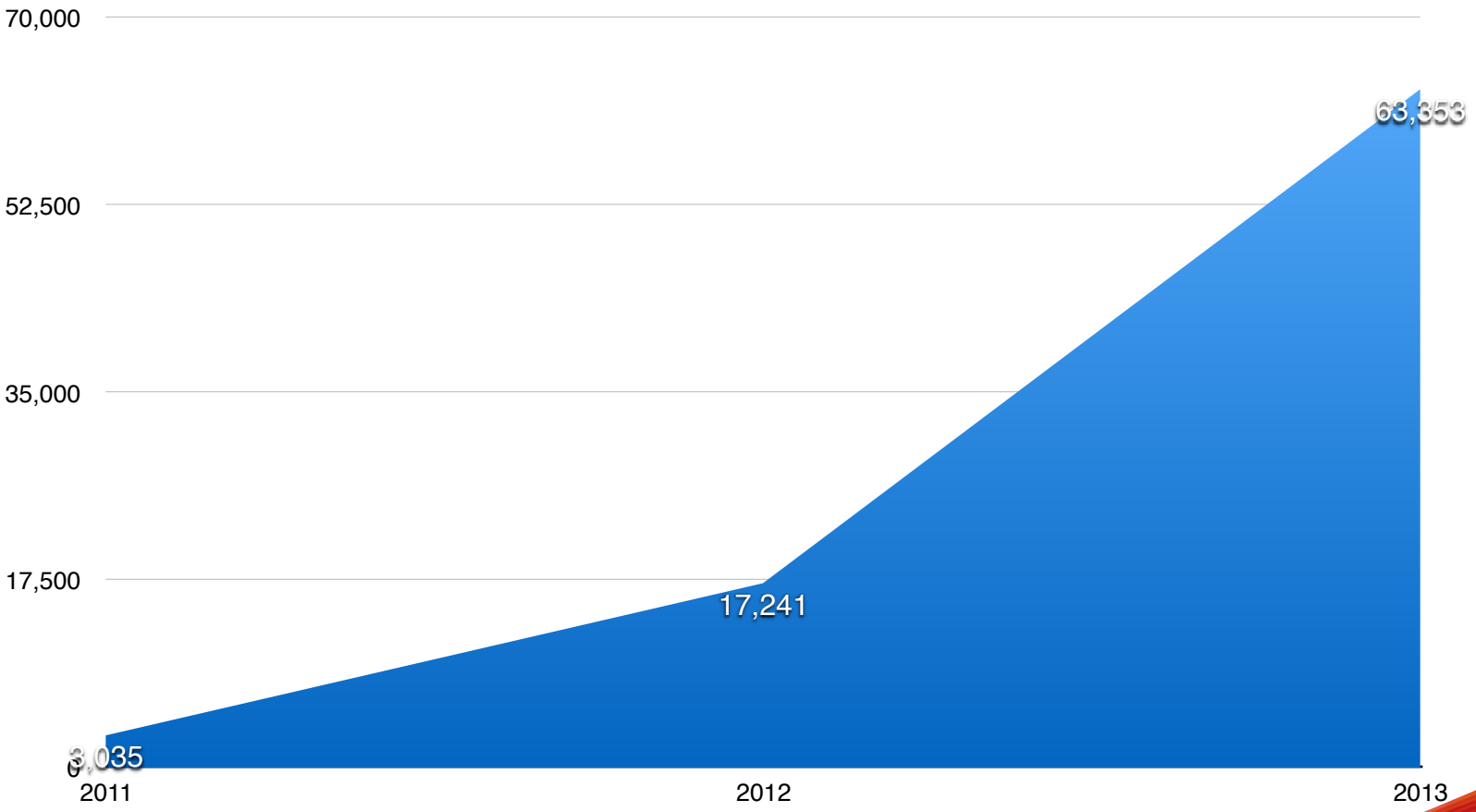
TRAFFIC

```
INVITE sip:000XXXXXXXXXXX@XXX.XXX.XXX.XXX SIP/2.0
To: 000XXXXXXXXXXX<sip:000XXXXXXXXXXX@XXX.XXX.XXX.XXX>
From: 1000<sip:1000@XXX.XXX.XXX.XXX>;tag=1ba25ae7
Via: SIP/2.0/UDP XXX.XXX.XXX.XXX:5070;branch=z9hG4bK-50489a18;rport
Call-ID: 50489a186c9c2ff6adacfcc8edb55af1
CSeq: 1 INVITE
Contact: <sip:1000@XXX.XXX.XXX.XXX:5070>
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, BYE.
User-Agent: sipcli/v1.8
Content-Type: application/sdp
Content-Length: 281

v=0
o=sipcli-Session 12278792 2114349621 IN IP4 XXX.XXX.XXX.XXX
s=sipcli
c=IN IP4 XXX.XXX.XXX.XXX
t=0 0
m=audio 5072 RTP/AVP 0 101
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=sendrecv.
```

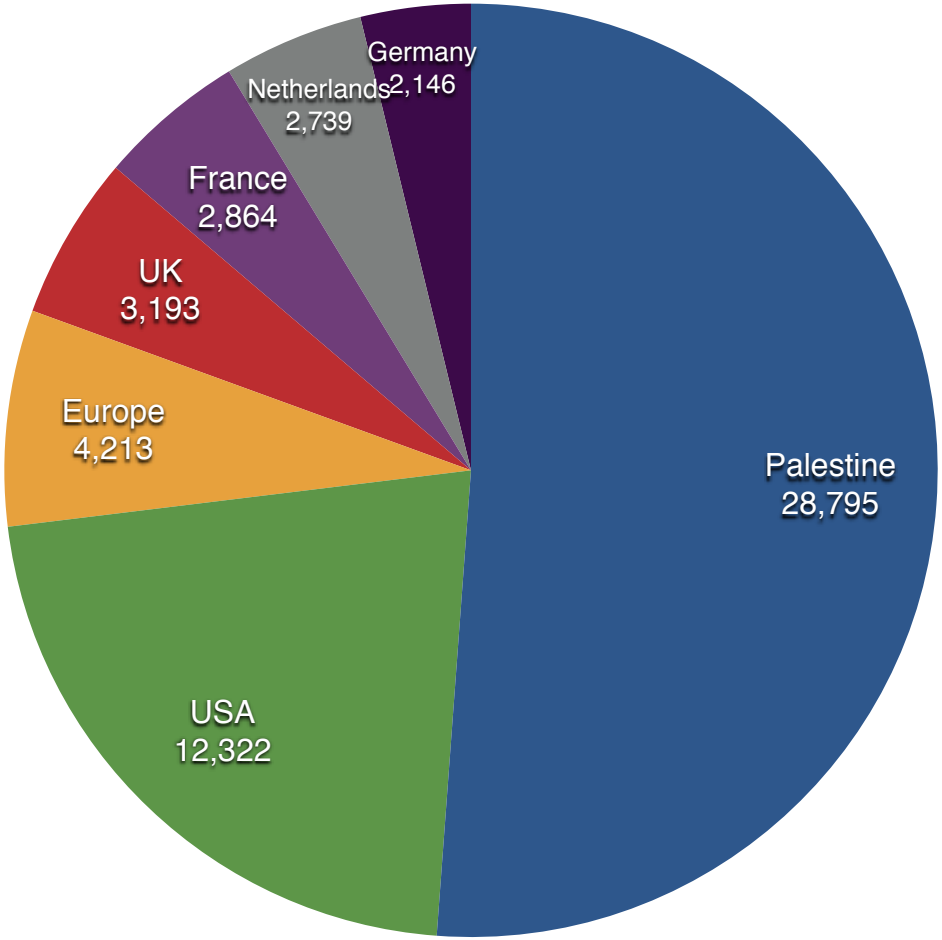
Simwood

TRAFFIC



Growth in call traffic (events by year)

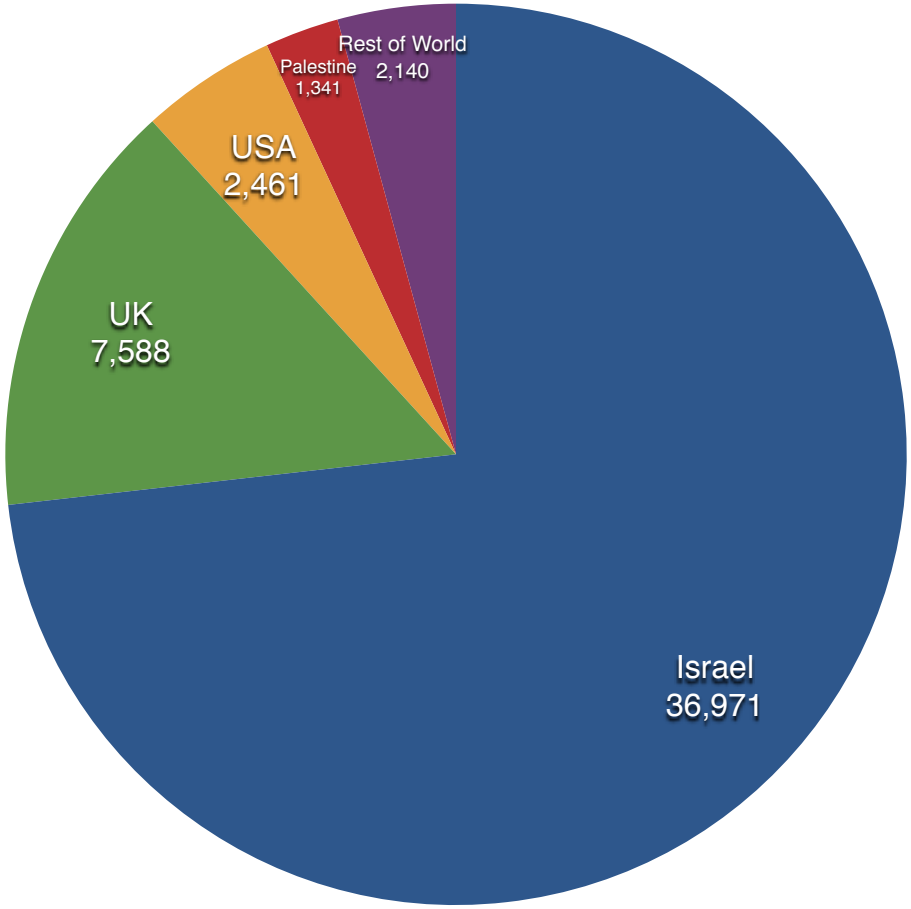
TRAFFIC



Sources of call traffic (12 months)

Test Traffic

TRAFFIC



Location of test numbers (12 months)

TRAFFIC

25%

of test traffic from **2** numbers

50%

from the top **10**

TRAFFIC

Mostly ordinary ‘landline’ numbers

TRAFFIC

Absent from commercial feeds

Reminder:

This is Test Traffic

TRAFFIC

The visible attack hasn't yet started

Live DTF Traffic

No-Cost Solutions

Bill frequently, monitor continuously

Buy with prepayment

(Where they can kill calls in progress when credit exhausted!)

Use a carrier with real-time billing & CDRs

Use honeypot data

http://mirror.simwood.com/honeypot

SOLUTIONS

99.79% of 64m intrusions use the user agent "friendly-scanner"

Use TLS

(Or at least TCP)

SOLUTIONS

Avoid auto-provisioning

(Or at least filter by user agent, rate limit and log!)

Monitor & control off-net

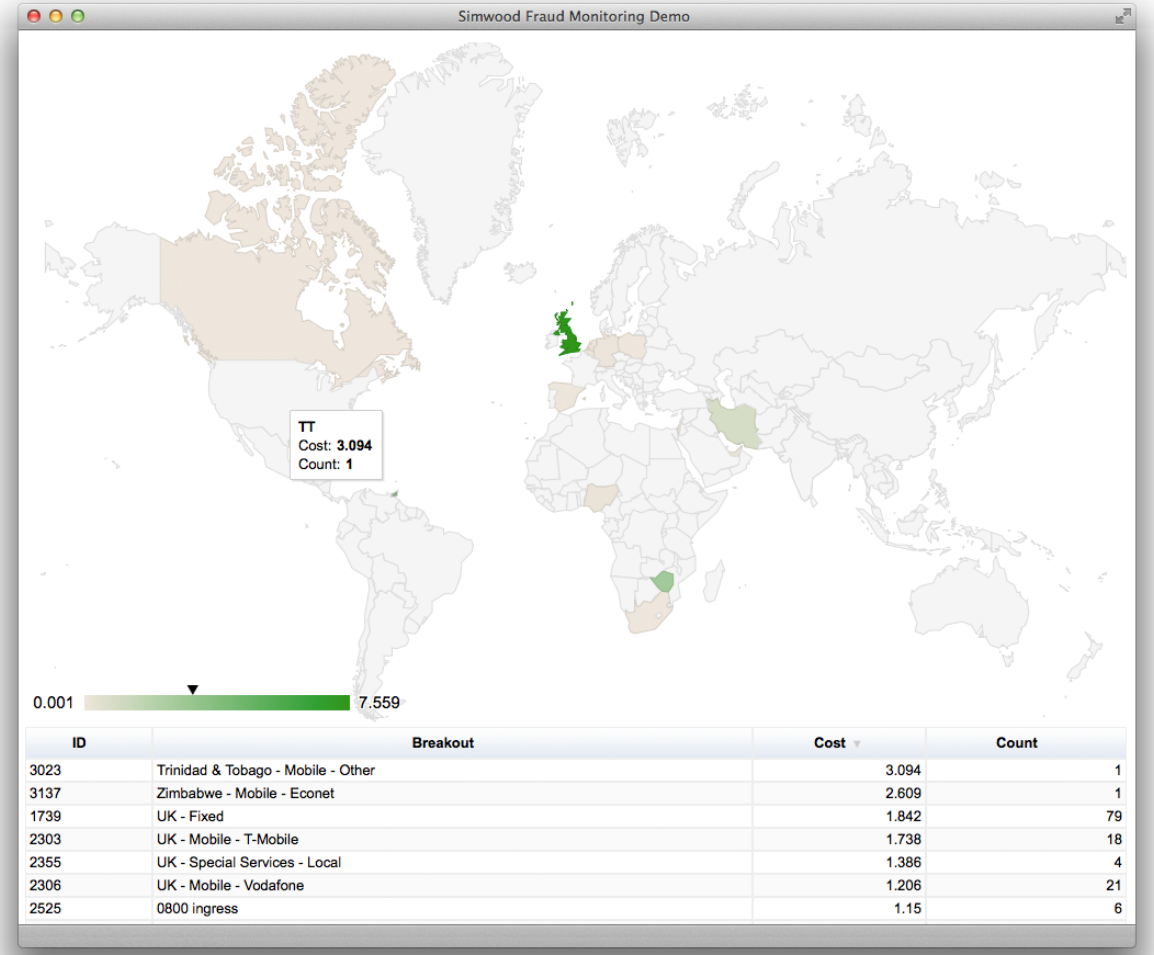
Example 1:

Value of calls *in progress*

Simwood

SOLUTIONS

MONITOR & CONTROL OFF-NET



ID	Breakout	Cost	Count
3023	Trinidad & Tobago - Mobile - Other	3.094	1
3137	Zimbabwe - Mobile - Econet	2.609	1
1739	UK - Fixed	1.842	79
2303	UK - Mobile - T-Mobile	1.738	18
2355	UK - Special Services - Local	1.386	4
2306	UK - Mobile - Vodafone	1.206	21
2525	0800 ingress	1.15	6

Max cost *per call*

Custom ACL

Channel limits

Overall, international, per destination number & known-hotspots

Rate limits

Overall, international, per destination number & known-hotspots

Automated alerts

API control

SOLUTIONS

MONITOR & CONTROL OFF-NET

All above features are available through the Simwood API **today**

DOES IT SCALE?

300,000 operations per second can't be wrong!

FINAL THOUGHTS

Fraud is the number 1 risk to VoIP businesses.

FINAL THOUGHTS

Manage risk not margin. Voice is becoming a feature not a service.

FINAL THOUGHTS

Let a competent carrier take the strain.

KEEP IN TOUCH

http://blog.simwood.com

@simwoodesms

Hardcopy in foyer

https://simwood.com/kamailio