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

Operator
Carrier
Wholesaler
Reseller
Retailer

Cost
Profit

Loss
TOLL FRAUD & DIAL THROUGH FRAUD

Operator: PRS Outpayment
Carrier
Wholesaler
Reseller
Retailer

Cost
Profit
Outpayment
TOLL FRAUD & DIAL THROUGH FRAUD

- **Operator**: PRS Outpayment
- **Carrier**: Cost, Profit
- **Wholesaler**: Cost, Profit
- **Reseller**: Cost, Profit
- **Retailer**: Cost, Profit

**Profit to Fraudster** → **Loss**
COMMERCIAL PRESSURE

VOICE IS BECOMING A FEATURE, RATHER THAN A SERVICE

THE WISE MINIMISE RISK, RATHER THAN MAXIMISE THEORETICAL MARGIN
60 minutes in the Simwood Darknet on a Sunday afternoon
http://mirror.simwood.com/honeypot
KEY INTRUSION METHODS

SIP Scan

Stage 1: Reconnaissance
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
Growth in reconnaissance traffic (events by year)
KEY INTRUSION METHODS
SIP SCAN

Sources of reconnaissance traffic (12 months)

- Germany: 644
- USA: 529
- UK: 56
- Other: 165
SIP Scan

Stage 2: 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
KEY INTRUSION METHODS
SIP SCAN

Growth in scan traffic (events by year)
KEY INTRUSION METHODS

SIP SCAN

Sources of scan traffic (12 months)

Germany
47,803,899

USA
6,194,621

UK
2,944,596

Anonymous Proxy
2,453,447

Thailand
2,135,810

Republic of Korea
569,708
Targeted Exploit
KEY INTRUSION METHODS

Auto-provisioning
INVITE sip:000XXXXXXXXXXXX@XXX.XXX.XXX.XXX SIP/2.0
To: 000XXXXXXXXXXXX@sip:000XXXXXXXXXXXX@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: 50489a186c9c2ff6adacfc8ed55af1
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.
TRAFFIC

Growth in call traffic (events by year)

- 2011: 0,035 events
- 2012: 17,241 events
- 2013: 63,353 events

www.simwood.com
Sources of call traffic (12 months)

- Palestine: 28,795
- USA: 12,322
- Europe: 4,213
- UK: 3,193
- France: 2,864
- Netherlands: 2,739
- Germany: 2,146
Test Traffic
Location of test numbers (12 months)
25% of test traffic from 2 numbers
50% from the top 10
TRAFFIC

Mostly ordinary ‘landline’ numbers
Absent from commercial feeds
Reminder:
This is Test 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
99.79% of 64m intrusions use the user agent “friendly-scanner”
SOLUTIONS

Use TLS

( Or at least TCP )
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*
SOLUTIONS
MONITOR & CONTROL OFF-NET

(simulated data)
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.
Let a competent carrier take the strain.
KEEP IN TOUCH

http://blog.simwood.com
@simwoodesms
Hardcopy in foyer

https://simwood.com/kamailio