

A LOOK BACK AT 9 YEARS OF FRIENDLY SCANNING AND VICIOUS SIP

Sandro Gauci - [Enable Security](#)

\$WHOAMI

- Behind *Enable Security (GmbH)*
- We do Pentests!
- VoIP / Communications / Network / Infrastructure / Web Application / WiFi / Software products

NEXT ~30 MINUTES

- How and why SIPVicious was published
- Reactions (cybercrime and security hardening)
- What's next?

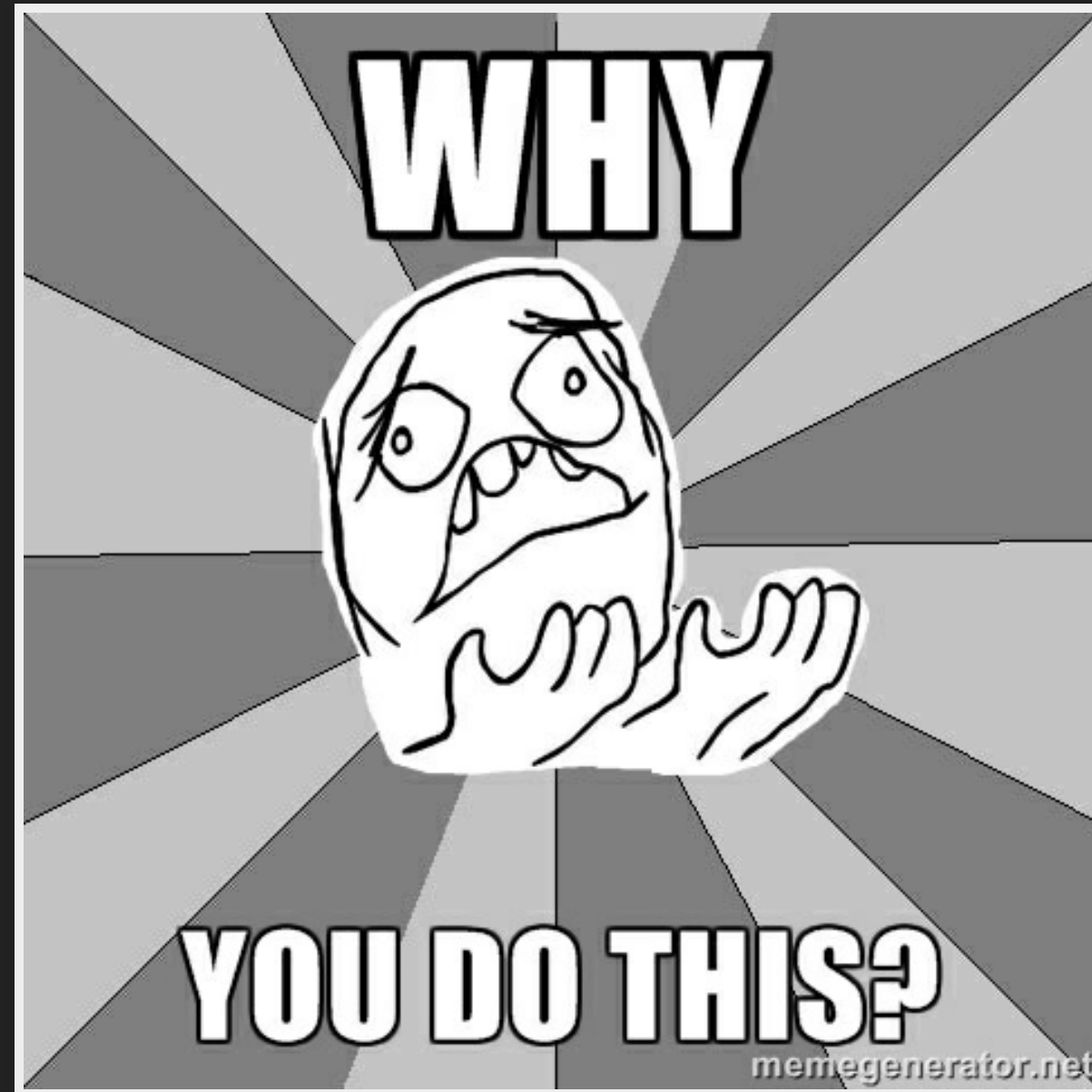
HUMBLE BEGINNINGS

- pentest on a PBX product for a software vendor 2007
- tools back then were mostly proof of concept
- no online password cracker (apart from THC Hydra)

MAJOR SECURITY ISSUES WITHIN THE PBX ON TEST

- product on test was generating extensions starting from 100 with the password as the extension
- not an isolated case
- guessing the user/pass often meant *free* long distance

WHY DO THIS?



LET ME STATE THE REASONS

- ease of setup
- especially with hardphones
- no security tools to demonstrate how bad this is

SIPVICIOUS WAS BORN

- initial code was just to demonstrate to client
- eventually shared the code with other pentesters
- got to a level where it was useful to others

SVCRAK

SVWAR

"If the Request-URI indicates a resource at this proxy that does not exist, the proxy MUST return a 404 (Not Found) response."

- rfc3261

SVMAP

"All UAs MUST support the OPTIONS method." - rfc3261

THE PUBLISHING!




SUNDAY, JULY 29, 2007

SIPVicious tools for auditing SIP devices

SIPVicious tools version 0.1 have been uploaded on [googlecode](#). These tools allow you to launch brute force password guessing attacks on PaBXs, identify SIP devices, softphones and hardphones on the network and guess live extensions on a PaBX.

Any feedback is welcome, tho some feedback is more welcome than other feedback ;-)

Download the latest (and earliest) version [here](#).

POSTED BY SANDRO AT 10:50 AM 

LABELS: SIPVICIOUS TOOLS

by

ENABLESECURITY

DOWNLOADS

[SIPVicious](#)

[TFTP Theft](#)

RESOURCES

[SIPVicious video intro](#)

[Our snort rules](#)

[Storming SIP Security](#)


[Getting started with SIPVicious](#)

*published 29th July 2007 and had instant
feedback from other security
researchers/pentesters and eventually, VoIP
community*

*met a lot of friends both from the security
and also the VoIP community*

MALICIOUS USE

I SEE WEIRD EMAILS

THANK YOU 



afk@jungle.net <afk@jungle.net>

8/7/08 

to me 

THANK YOU FOR MAKEING PUBLIC SIP VICIOUS SCANNER.
I USE IT 24/24 SINCER 04 OF 2008.
IT'S GREAT!

thank you!

yours Paul.



next dream <nextdreamnet@gmail.com>

3/4/10

to me ▾

Hello I need Help with the sipvicious i being trying please it is very important .


Regards


I await to hear from u


next dream

to Sandro Gauci [Show details](#)

Mar 5, '10 (6 years 2 months ago)

Archive 

 Reply

More 

Bro i would pay u man...lets work together please

[Show quoted text](#)



xml paypal <xmlcard@gmail.com>

3/18/10



to me ▾

Hello,

i am a user of **SIPVICIOUS** v0.2 and i would like to know if you have a new version or another program like it, to check the vulnerability of the SIP.

I can sponsor future projects.

Reply me ASAP.

Thank you.

user system <hima@ephonepremium.com>

3/1/11

to me

Hello sendro

Please i want now last update for SIPvicious
Send u money or any tread
Thanks
Im mohamed from egypt

weasdfa sfasdfsda <el3ashik100@gmail.com>

1/5/11 ↕

to me ▾

Hi man

i see your email in sipvicious program

i want to call you online important please if you have msn or yahoo

give me your email its very very erjant

thanx

RUUS LOVE <keylexy@gmail.com>

3/8/11

to me ▾

can i ask about sipvicious , i need small help,
if can ofcourse

thanks

good day


))))))))))))))))))

For usage help make use of -h or --help switch.

And if you're stuck you can always contact the [author](#).

fawakeh fawaka <xfawakehx@gmail.com>

1/10/11

to me 

hi do you have any good copy of sipvicious? personal one

Today

Ġeņerāl Āħmēd would like to add you on Skype.

أرغب في إضافتك كجهة اتصال، Sandro Gauci مرحبًا يا

16:08

Block

Decline

Accept



Pay It Forward Internet Marketing - Bob P Wilson

Like Page



September 20, 2013 · ✱

Freelancing, Affiliate Freelancer September 20, 2013 at 07:25AM I NEED SOMEONE TO CREATE ME A SIP SCANNER - repost by dolcesalon I need a unix based program (scanner) wich gets pbx info user password and sip usernames, ip and passwords (!) something like [sipvicious](#) but BETTER like state of art better . if it gets root username and password also along with the sip credentials is even better... (Budget: \$250-\$750 USD, Jobs: Anything Goes, Linux, PHP, Software Architecture, UNIX)
<http://bit.ly/19noWmu>

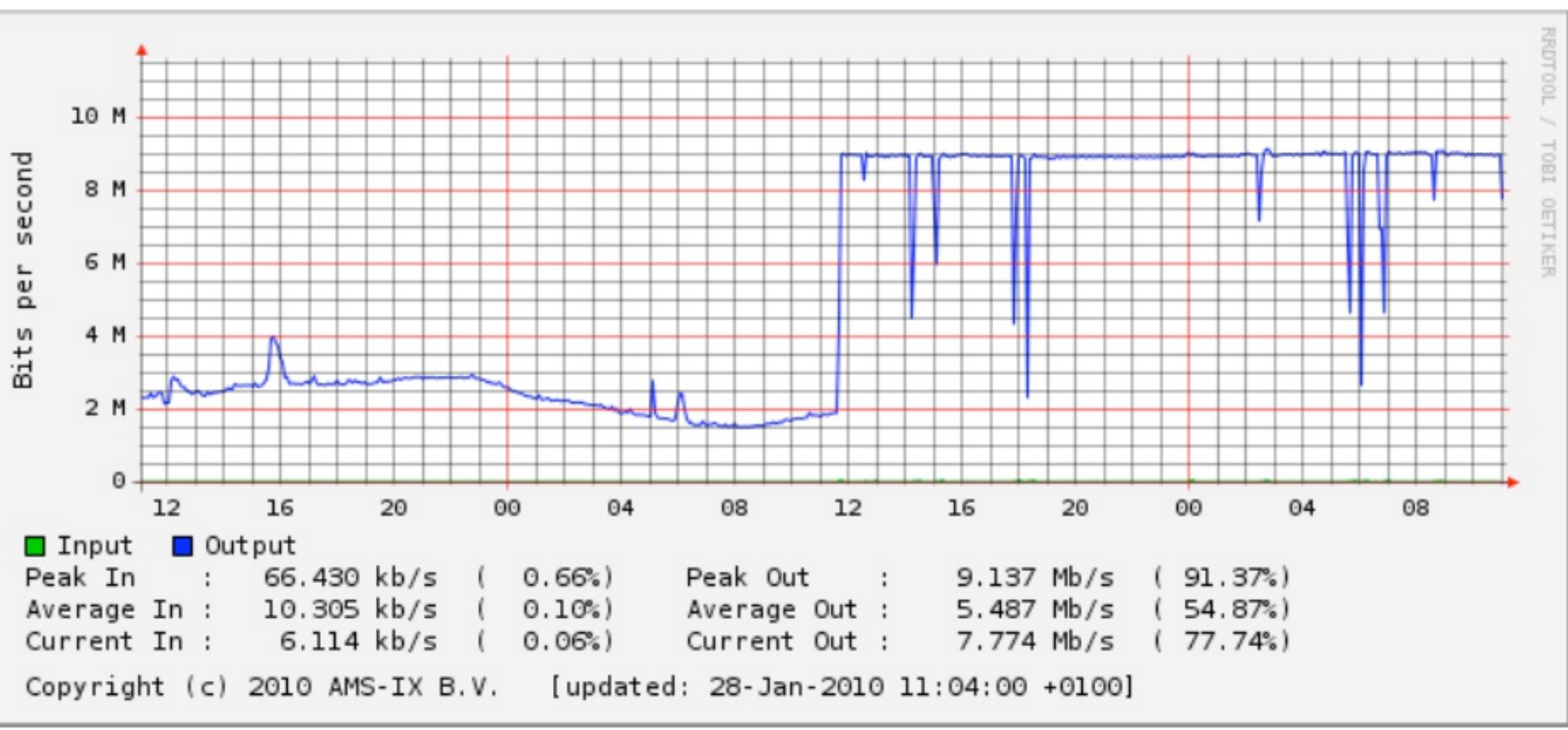
Like

Comment

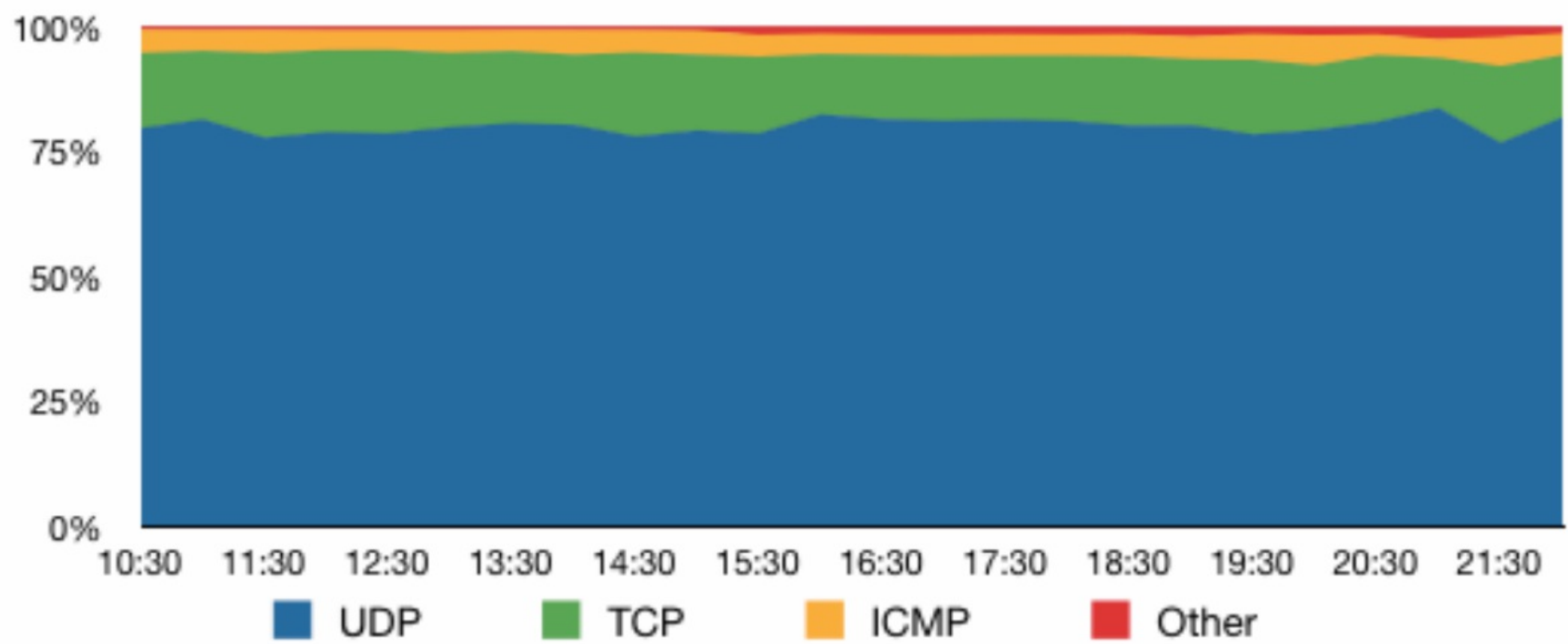
Share

FEB 2010: RIPE'S POLLUTION IN 1/8

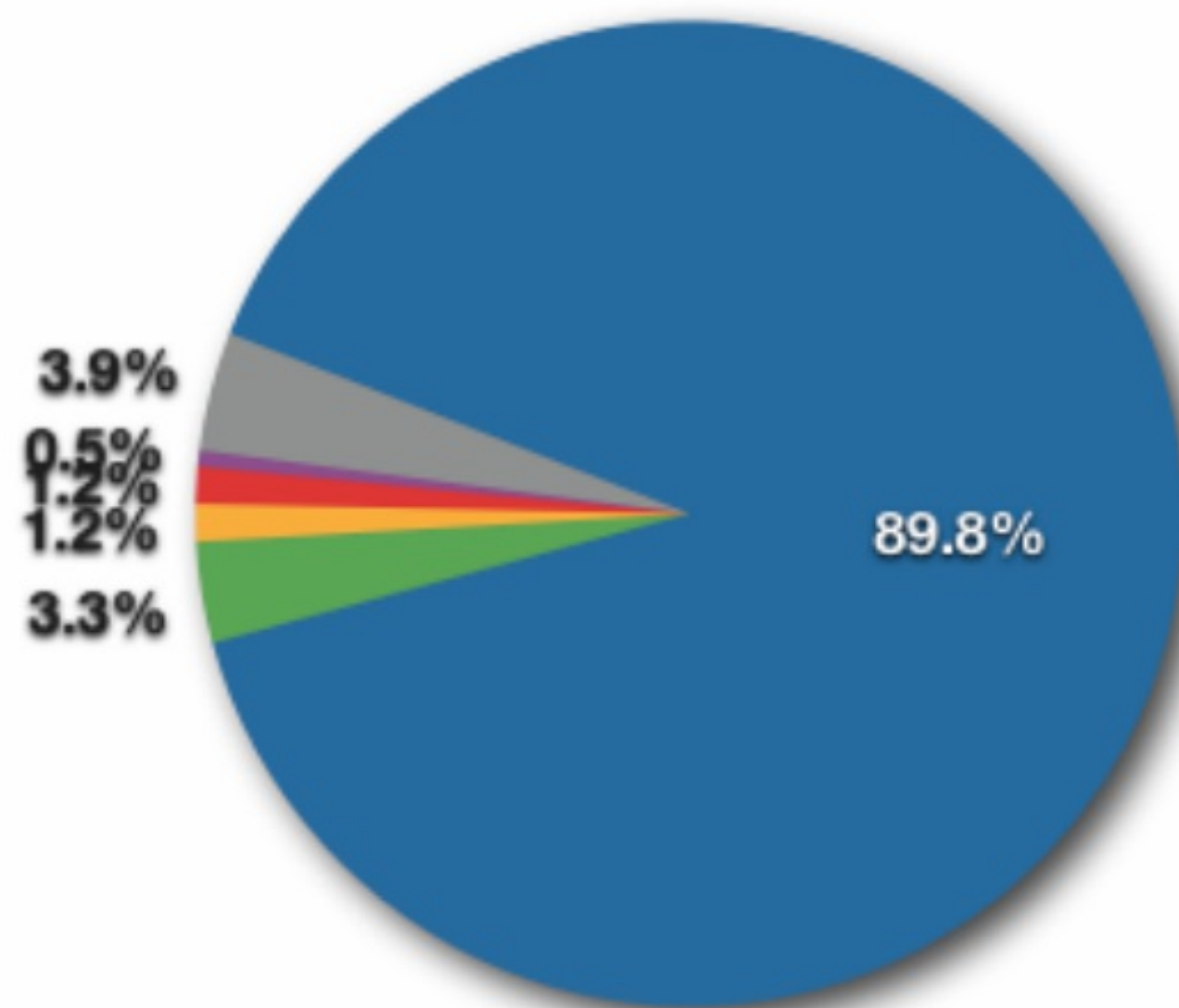
- on 2010-01-27 RIPE started announcing 1.1.1.0/24
- Only 10 MBit port
- It was maxed out immediately



Percent of Packets Over Time

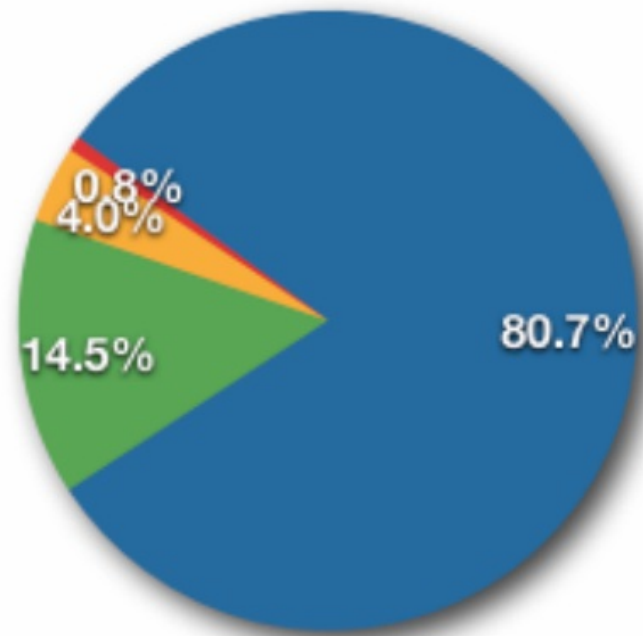


Destination Addresses in 1/8 (Percent of Packets)



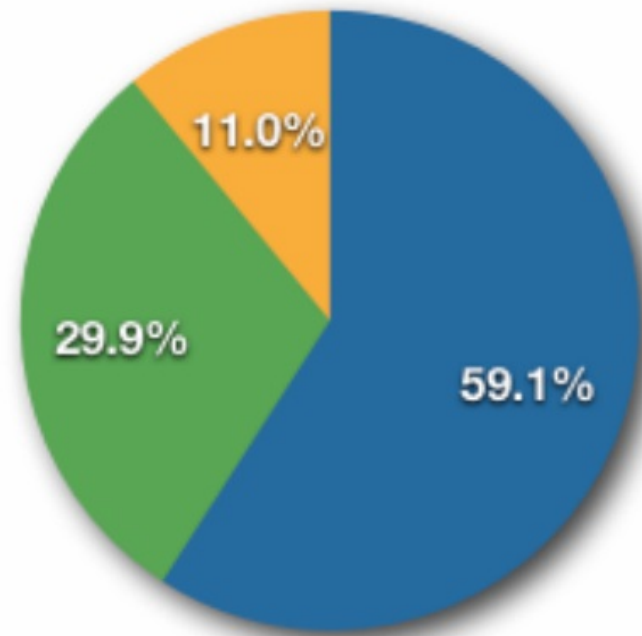
- 1.1.1.1
- 1.2.3.4
- 1.1.1.2
- 1.1.1.3
- 1.1.1.4
- Other

Traffic in 1/8



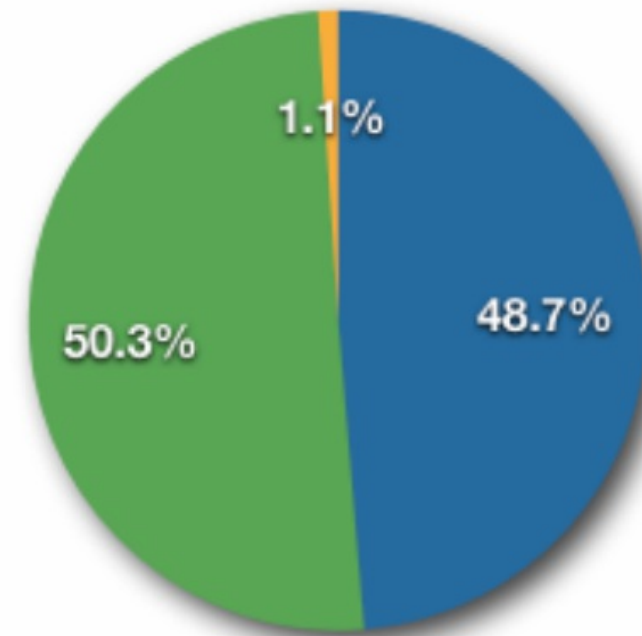
- UDP
- ICMP Traffic
- TCP
- Other

UDP Traffic in 1/8



- Port 15206
- Media Gateway Control Protocol
- Other

TCP Traffic in 1/8



- Attempted HTTP connections
- Other
- "Established" HTTP connections

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.”

```
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

THAT SDP AND RTP

- RTP (almost) always starts with an 0x80
- If an INVITE is accepted the RTP stream is sent to the IP in the SDP

**THROUGHOUT 2011:
SALITY PUSHED SIP
SCANNING TOOLS**

A Distributed Cracker for VoIP

0 votes

By: [Nicolas Falliere](#)  SYMANTEC EMPLOYEE

Created 15 Feb 2011 |  0 Comments

 0  29     Like  0

Back in the spring of 2010, I [blogged](#) about [W32.Sality](#) and the [decentralized P2P botnet](#) made up by hosts infected by Sality. The botnet is used to propagate URLs pointing to more malware. Recently, the gang behind Sality has distributed a tool to brute force Voice over IP (VoIP) account credentials on systems that use [Session Initiation Protocol \(SIP\)](#). SIP is a protocol widely used to initiate and control voice and video calls made over the Internet.

Let's rewind back to November 2010. At that time, a few [SIP-related blogs](#) and mailing lists reported attacks against SIP servers. The attacks consisted of *REGISTER* attempts using what appeared to be random account names. The novelty lied in the source of the attack, as it seemed the traffic originated from many different IPs. No specific malware was traced back to these attacks, though.

Recently, malware propagated by Sality caught our attention. It certainly stayed under our radar for a few months, and is the one that caused SIP administrators troubles last November. This malware, a distributed SIP cracker, is new in many aspects (there are known SIP crackers – tools or PoC, but no known in-the-wild malware, let alone one that implements SIP cracking in a distributed fashion.)

THURSDAY, NOVEMBER 4, 2010

Distributed SIP scanning during Halloween weekend

Over last weekend there were a number of reports of VoIP (especially Asterisk) servers that were "under heavy attack". I have looked at some packet traces and noticed how the SIP messages look very similar to the ones generated by SIPVicious especially swar.py. In fact, I think this is a modified version of SIPVicious that is being distributed on a botnet.

HACKERS PUSH SIPVICIOUS VOIP TOOLS IN MALICIOUS ATTACKS

by **Paul Roberts**

August 31, 2011 , 5:37 pm

Researchers at NSS Labs claim that they've spotted attacks that use Sipvicious, a common auditing tool for Voice over IP (VoIP) networks as part of malicious attacks aimed at taking control of vulnerable VoIP servers. The attacks are apparently aimed at taking control of VoIP servers to place unauthorized calls.

A description of the attacks, posted on the NSS blog on Wednesday, says that researchers at NSS have witnessed the Sipvicious tool installed by a Trojan downloader program on systems, most of which had first been compromised in drive by Web site attacks. The attacks use a known Trojan, jqs.exe, and connect to command and control servers to receive instructions on downloading instructions as well as the sipvicious tool from a .cc domain. After installation, Sipvicious is run and scan for SIP devices on the compromised computer's network and then to launch brute force attacks to guess the administrative password on those systems.

Related Posts

[SideStepper Allows for MiTM Between iOS Devices, MDM Tools](#)

March 31, 2016 , 10:41 am

[OS X Zero Day Bypasses Native SIP Protection](#)

March 25, 2016 , 8:15 am

[Chris Valasek Talks Car Hacking, IoT, at RSA](#)

March 14, 2016 , 12:29 pm

DEC 2012: TANDBERG COMPROMISES

REACTIONS

SVCRASH

TUESDAY, JUNE 22, 2010


How to crash SIPVicious - introducing [svcrash.py](#)

A new tool has been added to SIPVicious - [svcrash.py](#). As the name implies, it crashes something - [svwar.py](#) and [svcrack.py](#). This tool is meant to be used by system administrators and organizations that are receiving unauthorized scans on their exposed IP PBX.

Quick links: [Download the latest version](#) :: [Watch a short demo of \[svcrash.py\]\(#\)](#)

Klaus said...

Don't you think that attackers can edit python code to remove the timeout and handle the exception?

JUNE 24, 2010 AT 5:53 AM 

"Flooding VoIP providers doesn't do anyone good (granted that the attackers want free phone calls). Therefore the timeout added in SIPVicious version 0.2.5 is actually beneficial for both the victims and the attackers."

INDUSTRY REACTION

- alwaysauthreject in Asterisk and similar solutions on by default
- somewhat better passwords
- detection and blocking using fail2ban and similar

THE BIG REWRITE

Announced February 2012



WEDNESDAY, FEBRUARY 22, 2012

SIPVicious 0.2.7 released and rewrite coming up, looking for testers!

Get it now! This is the last release in the 0.2 series which fixes a number of stability issues and bugs before moving on to a total rewrite.

Are you a SIPVicious user? [Get in contact](#) if you have a VoIP lab or simply want to test the rewrite of SIPVicious. The internal version already includes support for TCP, TLS and IPv6 ;-)

by
ENABLESECURITY

DOWNLOADS

[SIPVicious](#)
[TFTP Theft](#)

RESOURCES

[SIPVicious video intro](#)
[Our snort rules](#)

WHY REWRITE THE WHOLE THING?

- Current code is exclusively UDP
- Not particularly neat, makes adding functionality hard

FEB 2012 PYTHON WITH GEVENT

- came across problems
- python3 needed a fork of gevent
- needed third-party library
- global interpreter lock
- only `svmap`

OCT 2012 NODE REWRITE

YET ANOTHER FAIL

- again, only svmap
- still not so reliable
- node and I did not get along so well

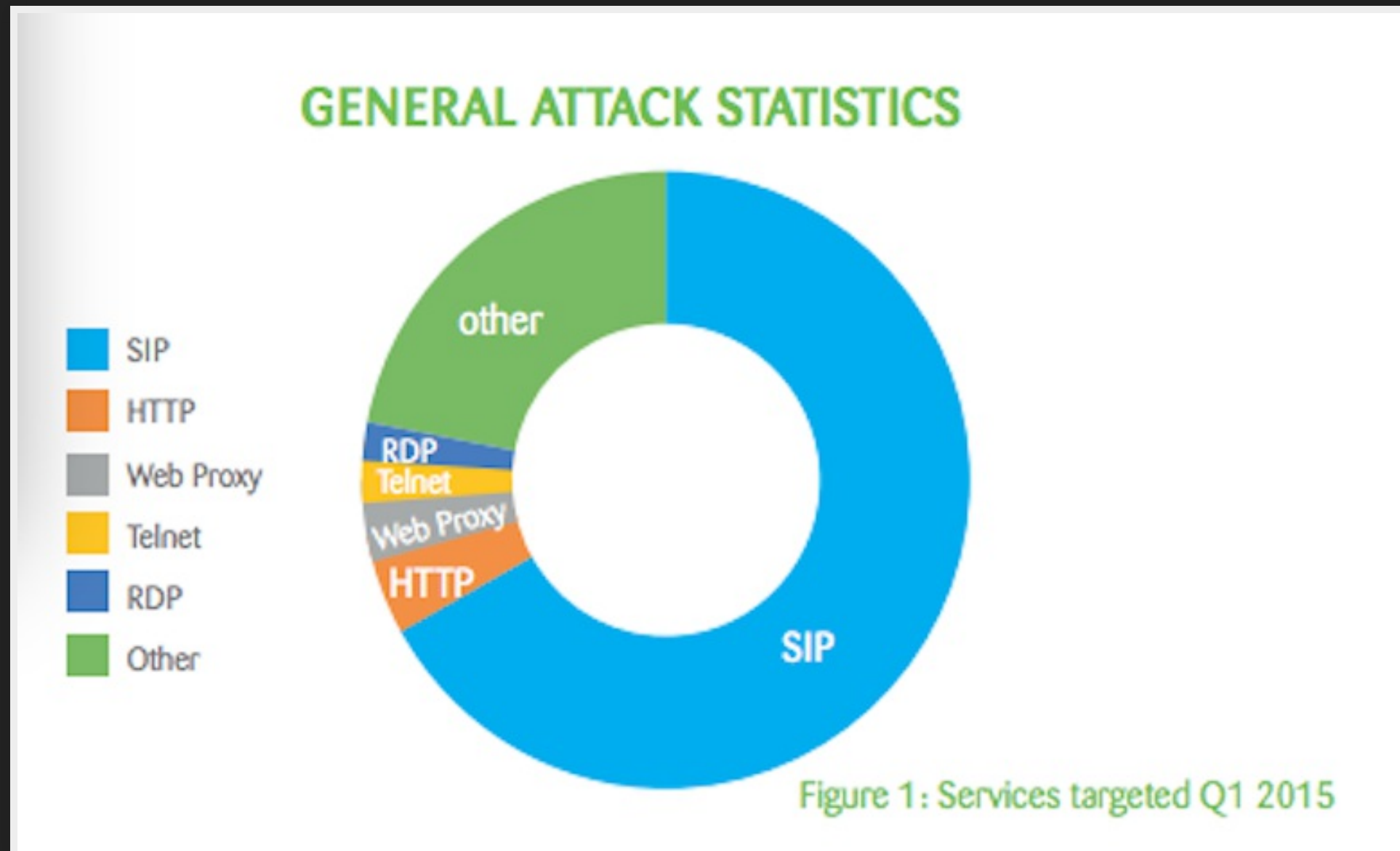
LESSON LEARNT

rewrites are not to be underestimated

SINCE THEN, I HAVE BEEN:

- using a combination of these tools
- plus SIP softphones (X-lite, Zoiper etc.)
- a custom small tools to automate certain aspects
- telling people that, the rewrite is not yet done
- a number of new security tools came out too e.g.:
 - Bluebox-ng
 - Viproy
 - vsaudit

June 2015: VoIP attacks are on the rise, particularly in the UK, according to new research by Nettitude



Tools	Occurrences	Percentage
friendly-scanner	71524	91.274%
sipcli/v1.8	6677	8.521%
eyeBeam release 1105a stamp 56793	76	0.097%
VaxSIPUserAgent/3.1	42	0.054%
IM-client/OMA1.0 sipML5-v1.2014.03.26	25	0.032%
eyeBeam release 3006o stamp 17551	10	0.013%
Custom SIP Phone	5	0.006%
SipClient 2.99	2	0.003%
cisco	1	0.001%
Total	78362	100.000%

FAST FORWARD TO 2016

- VoIP/comms pentests
- noticing an increase in usage of TLS
- SIP enumeration is often blocked
- Some vendors check the user-agent
- Passwords are still likely to be weak
- Enumeration may still be possible
- There are other attacks that need love ;-)

YET ANOTHER REWRITE

- tcp / tls / ipv6 support
- svwar working code
- svcrack on the way
- written in GO

WHAT ELSE IS NEW?

- Templates: which allow us to send all sorts of messages
- INVITE messages are handled properly (explain)
- New tool called svtest for individual specific tests
 - Can do in-dialog messages which reach behind the proxy
 - INVITE flood
 - SIP Digest Leak

DEMO OF EDITING OF TEMPLATES

DEMO OF SIP INVITE FLOOD

DEMO OF SIP DIGEST LEAK

**WHAT'S
NEXT?**

NOT YET PUBLIC

i.e. this is not an announcement

YOU TOO CAN HELP!

- hiring my company for your security testing ;-)
- making equipment available for testing
- feedback and ideas welcome
- testing the code (once available)

CONTACT

sandro@enablesecurity.com