Security Art | August 2011

Sounds Like Botnet

Itzik Kotler, Chief Technology Officer

Iftach Ian Amit, VP Consulting

www.security-art.com

Intro to VoIP

- It's everywhere
  - Home (Vonage, Skype, TeamSpeak, Comcast, etc…)
  - Office (Cisco, Avaya, Lucent, Asterisk, etc…)
- Easy to deploy
  - Most are "plug and talk" with fancy web interfaces to configure features such as voicemail, forwarding, conference calls, etc…

Overview of SIP

- Request/Response model
- Responsible for setup/teardown of voice/video calls
- Designed to allow “piercing” of firewalls, NAT, etc…
- Security? meh… (basic identification, usually not required in most PBXs, easily sniffed…)

VoIP as a Getaway Car

- So… VoIP can traverse firewalls easily
- And can go outside the corporate network over PSTN lines (no internetz needed…)
- And is rarely monitored (“can you hear me now” ain’t gonna pass through the DLP…)
- EXFILTRATE!

What is a VoIP Botnet

- Take your good ol'e botnet
- Disconnect all C&C channels
- Replace with VoIP
- Profit?

- Fully mobilized (NAT piercing)
- Looks more legit (try to pick THAT out of the traffic)
- Harder to peek into (can you spell "whazzzzup?" in RTP?)

Who Needs a VoIP Botnet

- Well, everyone…

- Botmaster is more mobile (literally)
- More anonymous C&C servers (conf call bridge numbers are aplenty…)
- Can actually transfer fair amounts of data back/forth (remember the modem days?)
- It's starting to show up as alternative methods of covert communications
  - Sorry spooks… ☹

VoIP Botnet in Action

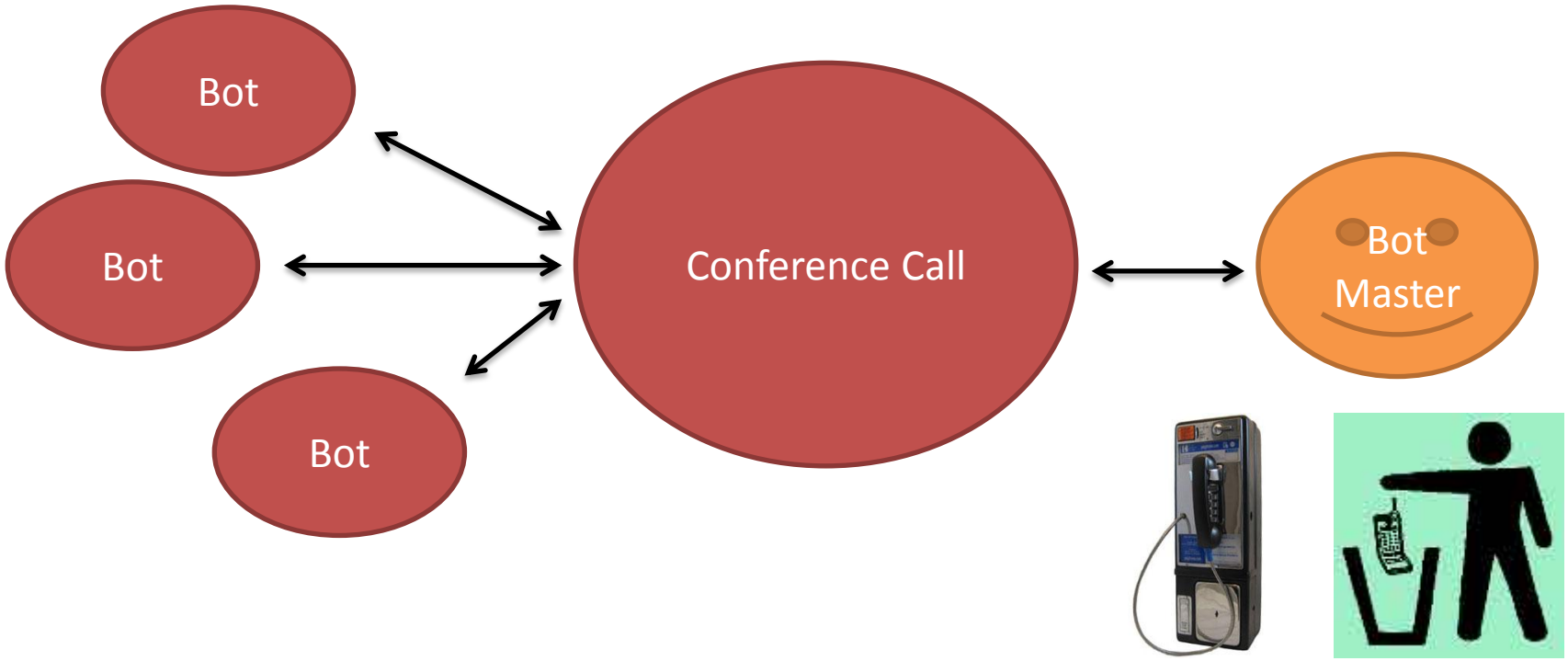
- Red Team Penetration Testing Engagement
- Botnet in No Internet/Closed Networks
- Botnet for VoIP Phones

VoIP Botnet Architecture

- Telephony systems allows both Unicast and Multicast communication
- Unicast:
  - Bot calls Bot Master
  - Bot Master calls Bot (registered ext. on his PBX)
- Multicast:
  - Bot A calls Conference Call
  - Bot B calls Conference Call
  - Bot Master joins Conference Call

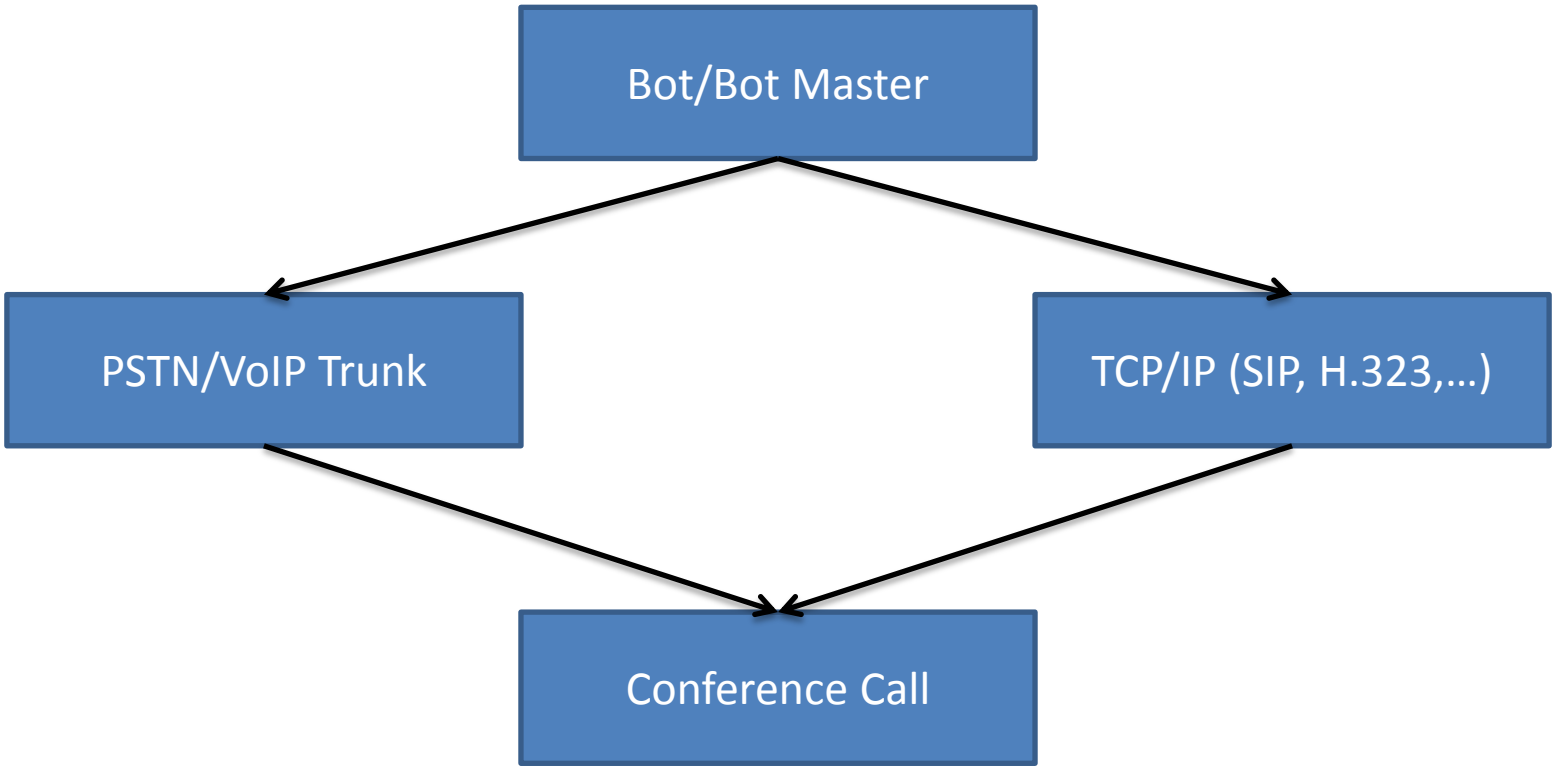
VoIP Botnet Architecture

- Conference Call as “IRC Channel”



The Call

- Calling can be made via TCP/IP or PSTN



Moshi Moshi

- Open-source VoIP Bot written in Python
  - Uses SIP as VoIP Protocol
  - Uses Text-to-speech Engines for Output
  - Uses DTMF Tones for Input

- Download your copy at:
  - http://code.google.com/p/moshimoshi/

Press 1 to Continue in l33t Speak

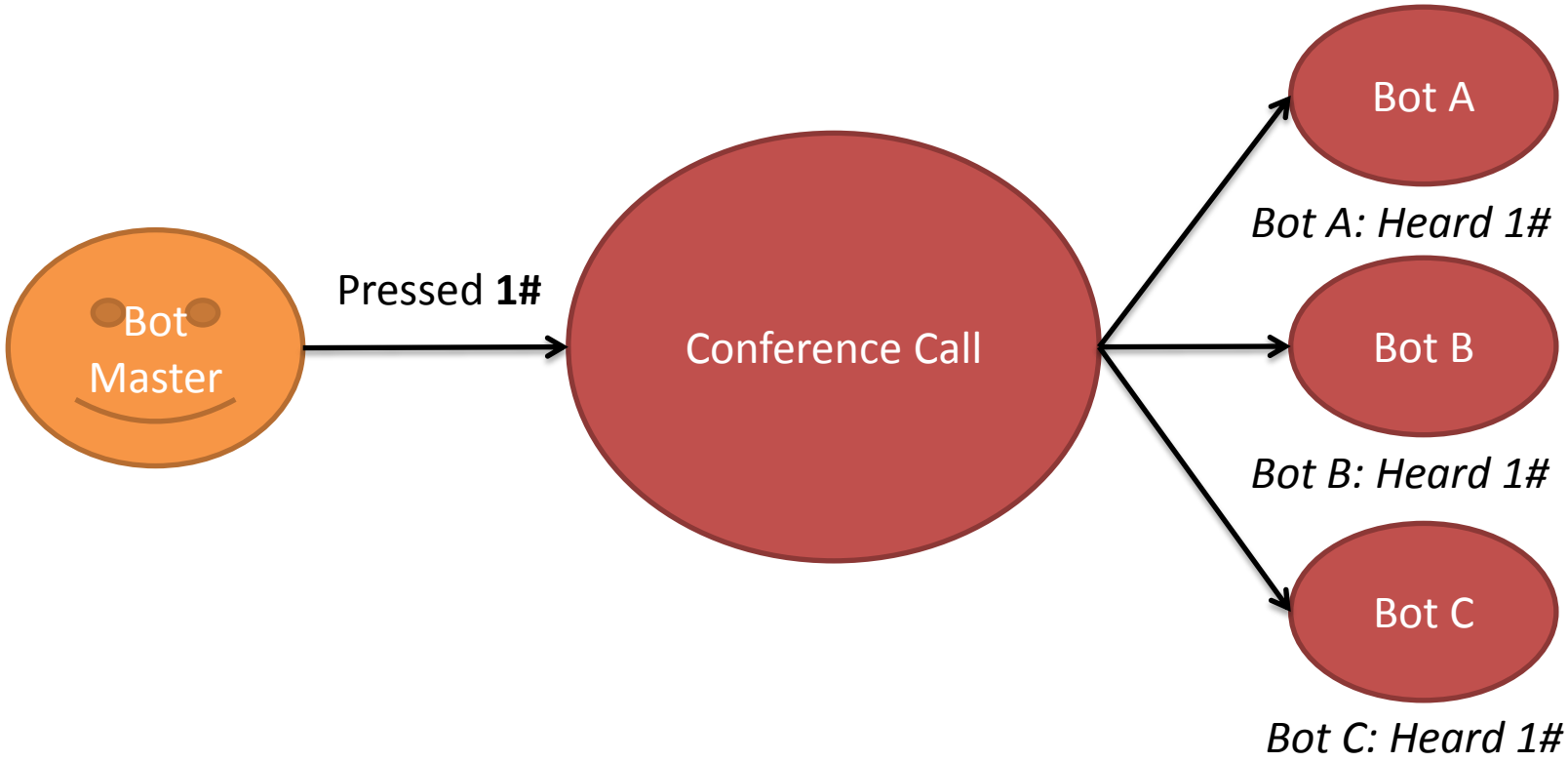
- DTMF (Dual-tone multi-frequency signaling) are used for signaling over telephone lines in the voice-frequency band between telephone handsets and other devices and switching centers.
- DTMF tones are standardized and can be sent and received from any phone

Asterisk as C&C and DTMF

- Asterisk is free software that transforms a computer into a communication server
- We're using ***AsteriskNow 1.7.1 Linux Distribution***
- MeetMe is a conference bridge for Asterisk and supports passing DTMF through the conference.
- To pass DTMF through the conference add '**F**' option to **MEETME_OPTS** at **extensions.conf**

DTMF Pass through/Relaying

- Conf. Call to relay DTMF to other calls



DTMF Tones as C&C

- The (made-up) Rules
  - ‘*’ is End of Line (EOL)
  - ‘#’ is a delimiter (i.e. Space)
- Examples
  - ‘0#*’ invoke command 0 without arguments
  - ‘1#123#*’ invoke command 1 with one arg ‘123’
  - ‘2#1#2#*’ invoke command 2 with args ‘1’ and ‘2’
- It’s your rules – go wild…

Ring, Ring!

Text-to-Speech as Data Leakage

- It's only natural that since we don’t have visuals in phone conversation, to use voice
- Passwords, documents, settings and acknowledgements can all be read back
- Some systems (Mac, Windows) includes built-in Text-to-Speech engines, others requires installation
- External utilities can be used to convert different formats (e.g. Microsoft Word) into simpler text files

Talk to me… Woo hoo!

The Getaway: Modulation

- Take any arbitrary binary data
- Devise a way to transform bytes to sounds
  - PoC: every ½ byte → one of 16 octaves within the human audible range (~200Hz - ~2000Hz)
- Record each ½ byte octave
  - PoC uses ½ second tones (for legibility in a conference ☺)
- Music to my ears…

Demo: Binary Data Modulation -> Data Exfiltration

- Transform data to sound
- Dial, leave a message…
- Transform recorded message to data
- Profit?

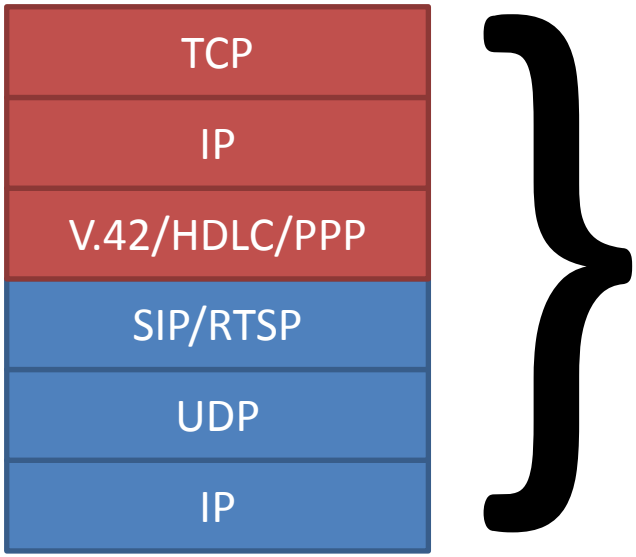
ET Phone Home!

VoIP as VPN

- Alternative unmonitored Internet access
  - No DLP
  - No Firewalls
  - No IDS/IPS/DPI
- Allows using already-existing C&C protocols
  - IRC
  - HTTP
- Bot Master can easily explore his Botnet
  - nmap –sS 10.0.0.0/8

TCP/IP over VoIP

- Bring back Modems to the game
- Use V.42/HDLC/PPP protocols



- Works with Hardware Modems
- Works with Software Modems
- Works within Voice frequency band
- Works under poor connectivity conditions
- Two-way communication channel

Did You Hear That?

- VoIP Botnets are as good and even better in some cases, than IRC, P2P, and HTTP Botnets.
- VoIP Botnets strengths:
  - Can be operated from a payphone, or a Mobile.
  - Can be accessed from both PSTN and Internet
  - Are not blocked by your typical IDS/IPS signatures

Countermeasures

- Separate VoIP from Corporate Network
  - Yes, COMPLETELY!
- Monitor VoIP Activity
  - It's your data. Same as you do for web/emails…
- Consider whitelisting Conf. Call Numbers

The Future Sound of Botnets

- Hearing is Believing
  - Speech-to-Text as Input
- Going Mobile
  - Text-to-SMS as Output
  - SMS-to-Voice Calls as Input
- Meeting new Appliances
  - T.38 (Fax) as Output (e.g. “Screen Shots”)
- Meeting old Appliances
  - Modem (PPP) as Input/Output (e.g. “Internal VPN”)

Questions?

Itzik Kotler (itzik.kotler@security-art.com)

Iftach Ian Amit (iamit@security-art.com)

Thanks!

Itzik Kotler (Twitter: @itzikkotler)

Iftach Ian Amit (Twitter: @iiamit)