How we accidentally created our own:

RAT, C2 , ~~Botnet~~ Distributed Computer Network

Adam Compton & Bill Harshbarger

RAPID7

Me Me Me…

- Who/What am I?

- Simple answer:
  - Father/Husband/Son/Brother
  - Programmer/Pentester/Researcher
  - Hillbilly

BILL…….

- Who/What am I?

Sort of Boring Stuff

Agenda:

• Get over stage fright and get started…	DONE
• Talk about ourselves…	DONE
• Present agenda…	IN PROGRESS
• Present rambling story of our accidental and haphazard path to creating a sort of working RAT/C2/etc...	COMING UP NEXT
• Maybe talk about other stuff too…	MAYBE IF THERE IS TIME
• Take questions...	LATER
• Go get drinks...	LATER...DOWN STAIRS

More Boring Stuff

Basic Terminology:

- RAT
  - **R**emote **A**dministration **T**ool
- C2
  - **C**ommand and **C**ontrol
- Botnet
  - Ro**bot Net**work
- Distributed Computing Environment

Just a Bit More Boring Stuff

Common Functions:

- Encrypted Comms
- Upload/Download Files
- Exec System/Shell Commands

Once upon a time....

- Multiple pentesters
- Internal engagement
- No Internet access
- In separate rooms

Chat Program

Requirements:

- Server
- Client(s)

Actions:

- Client sends message
- Server receives message
- Server forwards message to other clients
- Other Clients receive message and display it

DEMO: Chat Program

Encryption

Options:

- SSH Tunnel
- SSL/TLS Wrapper
- Standard encryption (AES)

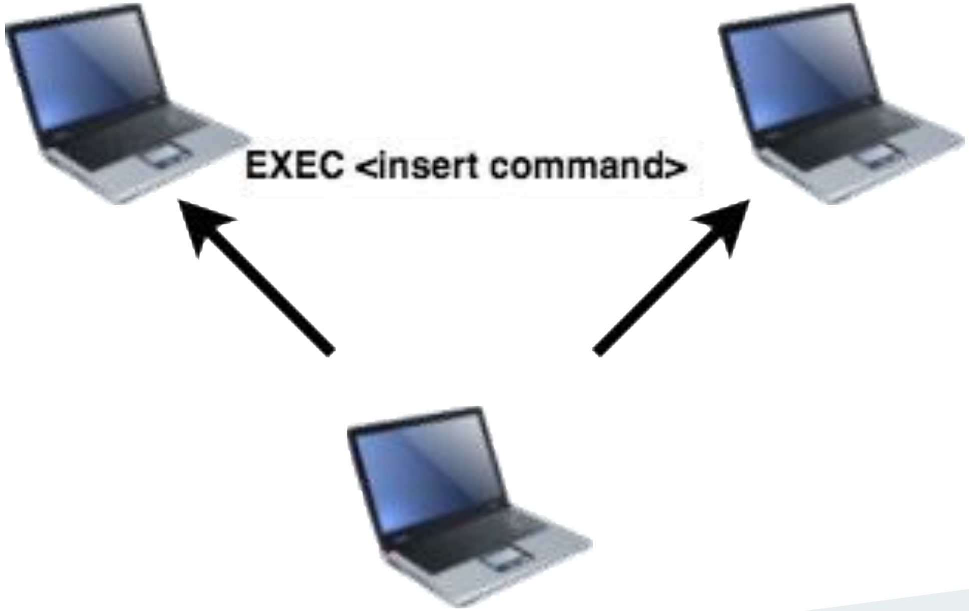
DEMO: Encryption

Remote Commands

TOM: Hey, run this command and give me the output.

BOB: I am not at my computer, I will do it later.

TOM: Never mind, I can run it without you!



DEMO: Remote Commands

File Transfer

Select file from local system

Send file securely to remote system(s)

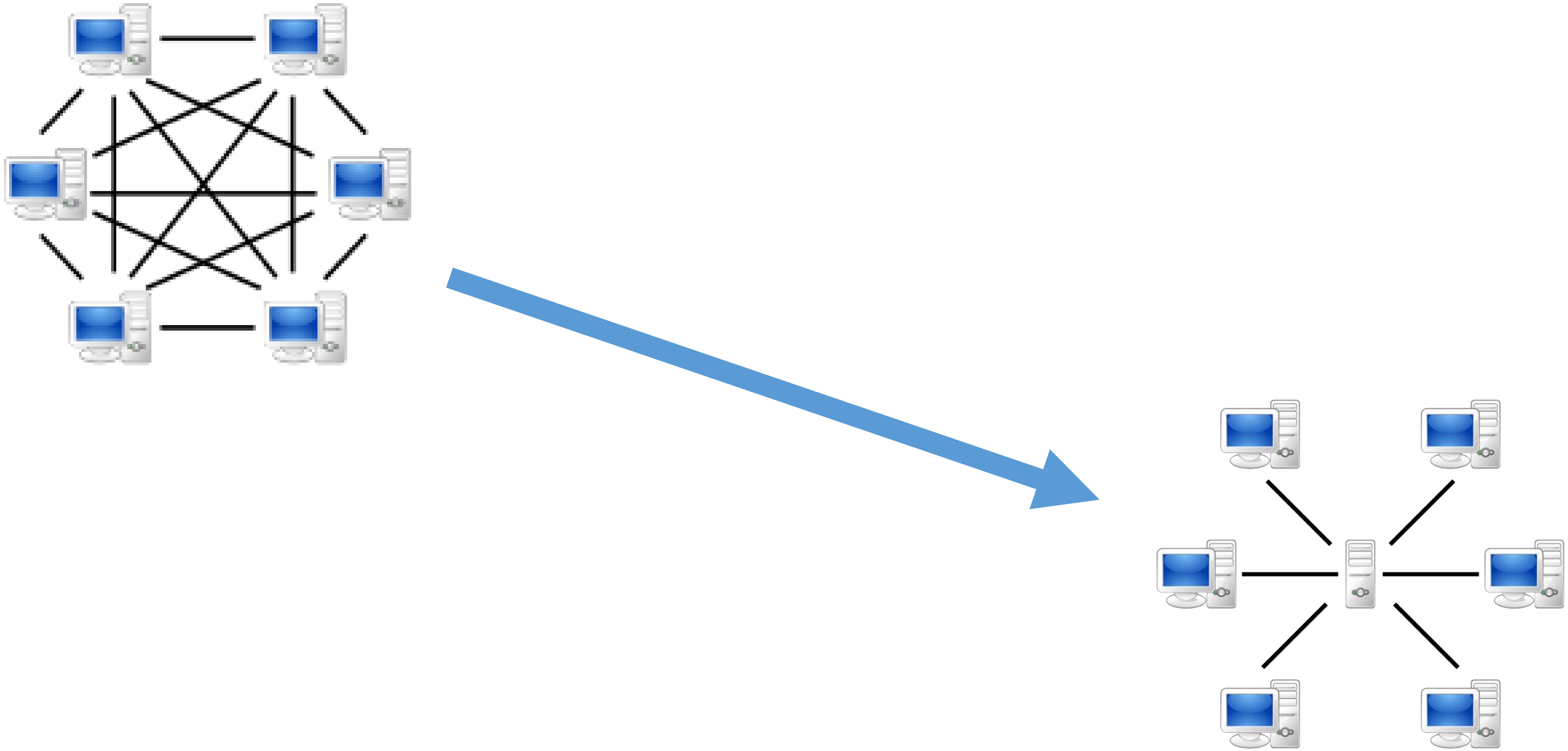
DEMO: File Transfer

Easy Deploy

It needed to be easy to install or deploy.

DEMO: Easy Deploy

Paradigm Shift



File Pull

DEMO: File Pull

Remote Shell

Fully interactive

DEMO: Remote Shell

Future Stuff

- Alternate communication channels/tunnels?
- SOCKS proxy

THANK YOU

Questions? Comments? Thoughts?

Contact Info:

- adam_compton@rapid7.com
- @tatanus

- bill_harshbarger@rapid7.com
- @