Botnet Tracking
by Freiling, Holz, Wicherski
ESORICS 2005

Presented by Bob Gilbert
24 January 2007
Doh!

What now?

IRC

Bots unite! Take down Oprah!

IRC

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?

Let's Party!

I'm getting bored

Next?
Questions this paper asks

- How to infiltrate botnet?
- How to prevent attacks?

Infiltration

- DNS/IP, port number of IRC server
- [Password to connect to server]
- Bot nick semantics
- Name of IRC channel [and password]
Check this out - It worked for me

Hmm, what have we here…

Ouch, that smarts!

Must … infect … others

Muah ha ha … doh!
Infiltration

• Vanilla IRC client probably not effective
  – C&C server stripped down - not RFC compliant
  – Analysis not scalable - too much log data
• Build own IRC client (drone)

(DDoS) attack prevention

• Contact owner of compromised bot and shut down
• Contact operator of C&C server and shut down
• Redirect C&C DNS resolution to IP in private subnet (DNS blackholing)

Results from analysis

• Analysis from Oct 2004 - March 2005
• 180 distinct botnets, 60 active in March
• 300,000 unique IPs joined
• Botnet size: 200 - 50,000
• Most executed commands:
  – Spread
  – Update
  – DDoS

mwcollect - honeypot alternative

• Capture malware in non-native environments
• Monitor multiple IP addresses
• Emulate a vulnerable service
• Analyze shellcode, download binaries
• Provide virtual filesystem
• Emulate shell

Questions?