

GhostNet

Mini-Botnets specialize in identity theft, fraud, and stealing corporate information

information  
and stealing corporate

# BOTNETS Evolution & Risk

NIKK GILBERT CISSP, CISM

**Botnets second to none when it comes to spamming**

5,000 videos on YouTube contain malicious links

# Bots and Botnets

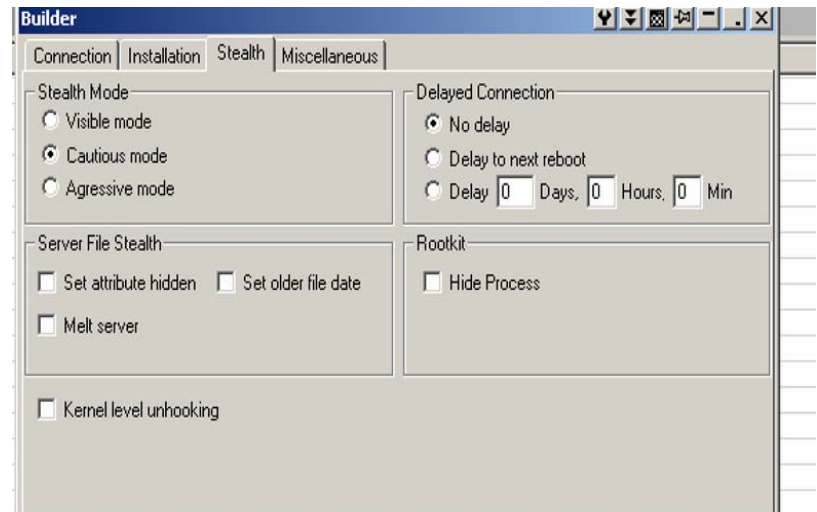
- ▶ A “Bot” is a type of malware which allows an attacker to gain complete control over the affected computer.
- ▶ A Botnet is a collection of these Bots which are centrally controlled.
- ▶ Common spreading techniques
  - Network shares
  - Instant Messenger
  - Unpatched systems or using known vulnerabilities,
  - Email attachments containing Trojans.
  - Malicious websites

# Evolution

- ▶ Spam: 120 billion Spam emails daily (58% of all spam)
- ▶ DDoS: Distributed Denial of Service Attacks (40Gb per sec)
- ▶ Identity theft
  - Installation of sniffing & key logging tools
- ▶ Hosting of illegal software with the enterprise
- ▶ Harvesting of software information
  - Product keys etc...
- ▶ Extortion, Social engineering
- ▶ Corporate espionage

# Bots now can be built in a Windows GUI

- ▶ Choose your base bot.
  - SDBot
  - GTBot
  - Agobot
- ▶ Configure Your Features
  - DDOS attacks
  - Keystroke logger
  - Credential collector
  - Spam
- ▶ Configure stealth level
- ▶ Finished



# Economics

- ▶ Billion Euro a year business
- ▶ 20 million valid email addresses cost \$1000
- ▶ Cost of the actual Bot program \$5–\$1000
  - Dependent on features
- ▶ Rent 10,000 bots clients 1 hour for \$200–Sophos
- ▶ .10–.25 cents per machine– Cisco
- ▶ Bot Masters are offering SLAs



# Where is the Risk

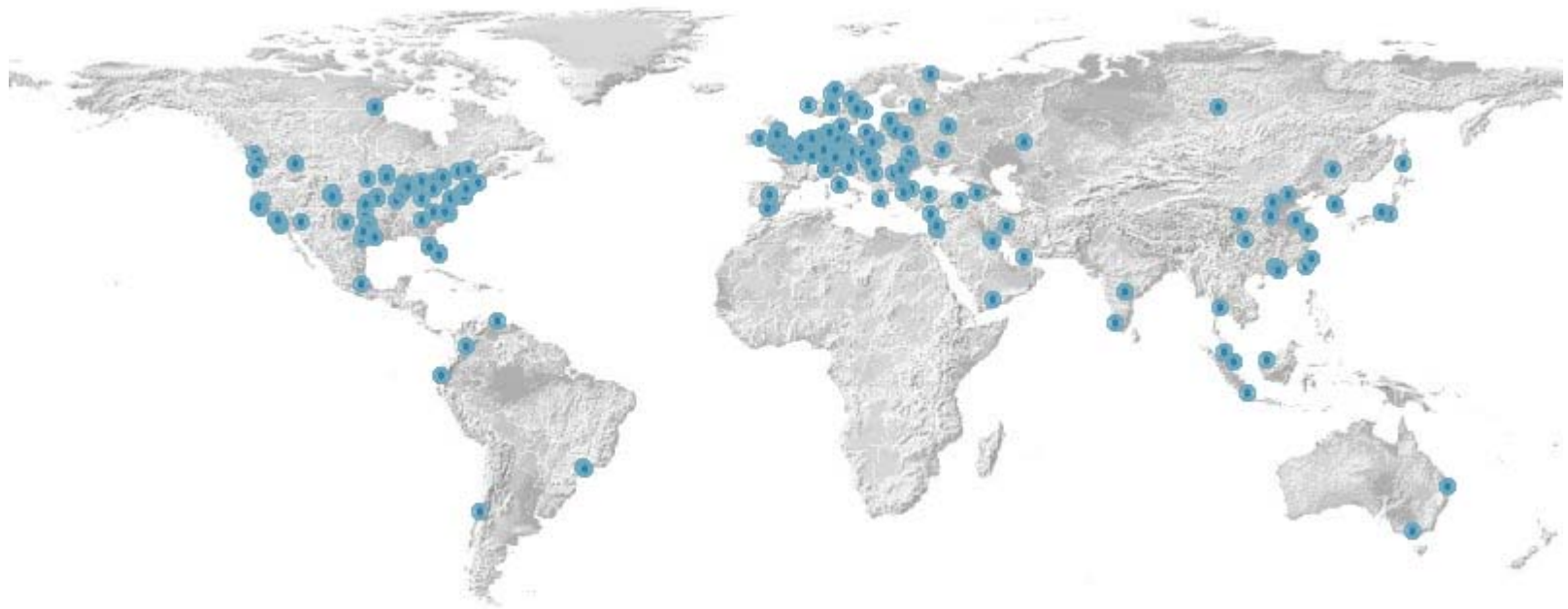
- ▶ 70% of the top 100 websites have hosted or been involved in malicious activity in the past 6 months. Websense
- ▶ 1 out of 10 computers infected with bots. Kaspersky
- ▶ 75% of enterprises will be compromised by Bot malware. Gartner
- ▶ 1 in 10 web pages are booby-trapped with malware. Google
- ▶ Top five Anti-Virus only 81% effective. SRI Threat Center
- ▶ Top Attacking countries using Botnets, Phishing & DDoS
  - United States, China, Germany, France and Russia



# Risk=

- ▶ Millions of Botnet crime victims identified. –FBI
- ▶ Ghost Network
  - GhostNet—infesting high-value diplomatic, political, economic, and military targets.
- ▶ Mini Botnets
  - Targeted attacks directed at specific organizations
- ▶ Cyber warfare
  - Botnets were used to knock out Estonia's & Georgian banking, internet etc... connectivity

# Location of Botnet Command and Control Servers Globally



# A Tough Defense

- ▶ Antivirus & IDS/IPS aren't completely effective against Bot infestations.
  - Why? Signature based.
- ▶ Botnets updated every 30 minutes to daily
- ▶ 1 out of 10 computers infected with bots. Kaspersky
- ▶ 75% of enterprises will be compromised. Gartner
- ▶ 3%–5% of enterprise network assets have Bot malware, even with up-to-date AV and other online defenses.

Damballa

# Mitigation techniques

- ▶ A good security policy
- ▶ Patching all desktops, servers
- ▶ Keeping network equipment up to date (Current IOS version)
- ▶ Strong firewall configurations
- ▶ Study of DNS traffic
- ▶ Disabling Autorun
- ▶ Limiting user admin rights on pc.
- ▶ Well managed Anti-Virus
- ▶ IPS/IDS with logging and follow up
- ▶ Web Security Gateways
- ▶ Content filtering
- ▶ Netstat -an



# Conclusion and Questions

