

# Evolution of Malicious IT Attacks

Clive Longbottom,  
Service Director, Quocirca Ltd

- Initially, viruses were just a way of techies showing off
  - Many did not directly impact the PC or its content
- Payloads emerged that deleted content
  - Some organisations found themselves being blackmailed
- It was found that the payloads could do other things
  - Send back information
  - Act as independent servers
  - Upload other function

- Nigerian 419 Scams
  - Spam-based direct payments or access to financial sites
- Key Recorders
  - Everything you type is sent back
- Phishing
  - Cloaked sites or redirects gaining individual details
- Individual to group
  - More “professional” approach for organised crime, dedicated cyber crime, terrorist or corporate spying groups

- OS vendors and discrete vendors fighting on many fronts
  - Anti-Virus
  - Anti-Spyware
  - Anti-Spam
- Dedicated teams uncovering possible vulnerabilities in OS, browser, applications
- Infiltrating user groups and “darkroom” forums to see what is being discussed
- Advanced approaches to stopping threats
  - Even before the threat is fully identified

- Multi-level, multi-approach threats
  - Phased code, capability followed by function
- Highly targeted approaches
  - Farming of individual information from social networking sites
    - No “bcc:” usage on spam
    - Cloaked/redirected sites pre-populated with some information (e.g. full name, address, age)

- USB and other add-on devices
  - Portable drives of up to 450GB
- Continued usage of P2P tools
  - Bypassing firewalls, downloading who knows what?
- Social Networking sites
  - Let me give you my name, address, mother's maiden name, pet's name
  - Let you give me a payload
- Access to easier tools for personalised working
  - Hey, look – I can see my desktop from my laptop!
- Lazy access
  - OOTB WiFi

- Strangle at birth
  - Multi-level approach to stop infection and entrapment
    - Stop the threat from getting on the network
    - Stop the threat getting to a client
    - Stop the threat from infecting
    - Stop the threat from spreading
- Fully dynamic need
  - The threats are changing, the solution must change as well
  - “Day 0” capability – use of heuristics and advanced matching algorithms to stop threats before they have been fully uncovered in the vendor community