Hostile attacks on UK Cyber Space

• HM Government National security strategy unveiled - Monday, 18 October 2010
• Where do the greatest threats to the UK’s national security come from?
• The most pressing of these, referred to as ‘Tier 1’ risks includes: hostile attacks on UK Cyber Space
• £350M Cyber spend UK Gov
BT Security Investigation

- Asset Protection
- Revenue Fraud and Crime Management
- Intelligence
- E-Crime Team

  Forensics

  Investigators

  CERT
What does BTCERT do?

- An investigation team, to co-ordinate all internal computer and network security incidents across BT, serving the specific needs of the BT community;
- Produce Internal Disciplinary Reports
- Support and represent BT within the FIRST and TF-CSIRT communities;
- Contribute to raising security awareness across the business at all levels;
- Work alongside other key areas, primarily SubCERTs, to ensure security for all IP related products and services marketed for E-business purposes;
- Provides BT’s link into other global CERT and CSIRT teams;
- Link into key areas such as Information Assurance as part of a wider incident management process.
- Link with Law Enforcement Agencies.
What does BTCERT respond to?

- Junk / Offensive email Received by BT
- Internal Misuse of BT's Internet Access
- Unauthorised Software
- Network Attack
- Major Network Attack (Critical UK national Infrastructure)
- Port Scanning by BT Own Use Systems
- Port Scanning Originating from a BT ISP Customer
- BT Information Appearing in Public Domain
- BT Web Page Defacement
- Junk / Offensive e-Mail Originating from a @BT.com domain
- Phishing
- Other
What is the benefit of BTCERT?

- Co-ordinate the collection, evaluation, and analysis of information available following a Security incident.
- Contributes to the mitigation strategy as part of a Pan-BT Team and facilitate the retention of evidence to enable ongoing investigation.
- Provide an on-call 24x7x365 response for major cyber security incidents.
- Work with Investigation Managers and the Forensic Team to resolve logical security issues.
- Co-ordinate interaction with the Sub-CERT community.
What is a Sub-CERT

• SubCERT status has been given to key areas of BT deemed extremely vulnerable to external and internal malicious attacks.
• SubCERTs therefore receive priority incident handling for cyber incidents.
• Full SubCERT status is also only achieved after a site has attained the high levels of security practice as specified under FIRST regulations for full members.
Phishing Statistics

- 364 sites recorded 2010-2011
  - 1 server compromised 5 times
  - 3 servers compromised 4 times
  - 5 servers compromised 3 times
  - 55 servers compromised twice
    - Lnk.in used 10 times
- 55 “redirect” sites
  - Where site redirects elsewhere
  - Once redirected site is closed down, code updated to redirect to a different site (often within minutes)
- 51.6% sites shut down in < 1 day
- 88.7% shut down within 1 week
Phishing
Comparisons of CERT Incidents Reported 2009-2011
Bringing it all together