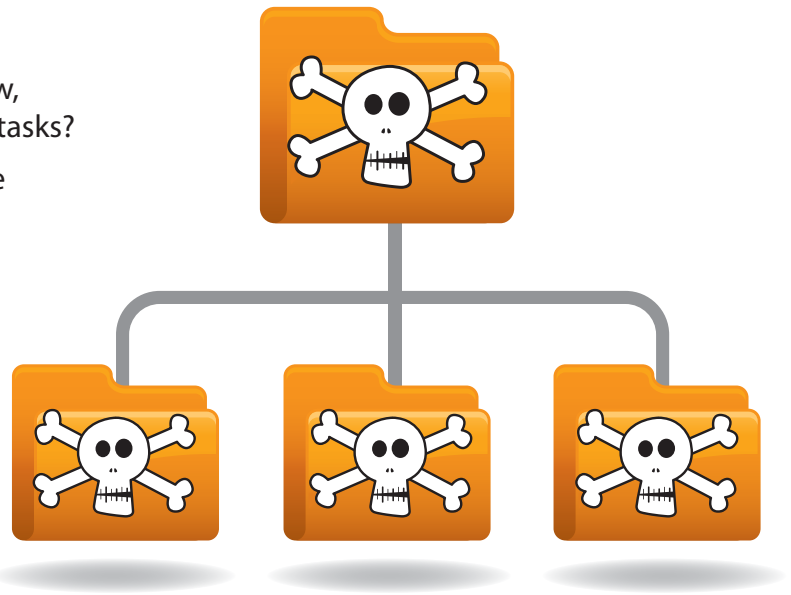


Zombies and Botnets

- Do you surf the internet?
- Does your computer seem unnecessarily slow, even when it is not performing any onerous tasks?
- Do you ever open attachments when you are unsure about the source?
- Do you copy data from external media i.e. memory sticks, CDs, DVDs?
- Do you or your staff use file sharing software?
- Do you watch video or listen to music online?

If you answered yes to any of the above questions then your business is at risk of infection from Bots & Zombies.



Description

Criminals and hackers use viruses and Trojans to exploit weaknesses in software code to gain access to computers and their processing power. The aim is to create a network of slave or 'Zombie' computers; this is called a 'Botnet'.

The Shadowserver Foundation, tracks Zombie numbers worldwide, and said it had seen at least a threefold increase in the last three months to 4th September 2008.

More than 450,000 computers are now part of zombie networks, or Botnets, run by hi-tech criminals. Criminals are keen to recruit new machines to a botnet to create a resource they can use or can be hired out to other gangs.

Most spam or junk mail is routed through 'zombie' machines forming a Botnet.

Source: <http://news.bbc.co.uk/1/hi/technology/7596676.stm>

CASE STUDY

Design Company, Manchester

'We just assumed that the computers were slow because of the internet connection and the specialist software we use. It never occurred to us that our computers had become Zombies!'

The company did not have any specialist ICT support, and it was only when an employee became so frustrated with the speed of her computer and looked online for a solution that she found out about Botnets, and became aware of the threat. The company hired an ICT Security Specialist to come in and investigate the problem and the problem was found and resolved.

'We were very fortunate only to have lost productivity through inefficient computers, it could have been much worse. However, being part of a Botnet for over four months has cost our company in terms of productivity and output. We now ensure that we have all the correct solutions, and most importantly, that all software is regularly updated.'

Solutions

- + If you think you have been already infected, seek professional advice. It may be that a loss in processing power is linked to insufficient memory or failing components, but it may also be that a computer is being used as a Zombie
- + Always use the viewing pane function within your email client, as opening a suspect email can execute malicious code designed to take over the computers processing power
- + If a suspect email is received, advise your ICT manager, and delete straight away
- + Use anti-virus software. Run automated scans at regular intervals. If concerned, run a manual scan
- + Ensure that all software receives automated regular updates
- + Use the most secure internet browser, such as the latest Microsoft Internet Explorer. This helps protect against sites that contain malicious code
- + Ban the use of file sharing software as downloads can often contain malicious code/viruses
- + Ban the use of social networking sites
- + If not required for business disable functions such as ActiveX and Java script. Seek professional advice to properly configure systems
- + Introduce an email and internet policy and train staff. Incorporate a short, but regular test to ensure policies are understood and followed
- + Introduce an ethical use policy that should be incorporated into terms of employment
- + Consider controlling the use of the internet. Setup an Intranet and allow access to sites required for business only
- + Always make sure you backup and that the backup is kept offsite. Regularly check that you can retrieve backed up files

Cost/Risk

- + The cost to the business of not taking the Bot threat seriously is often a loss in productivity, but the ramifications could be much more serious necessitating a system rebuild
- + The solutions are preventative in nature, but by their design, protect against numerous more destructive threats such as viruses & worms, and perhaps just as important – inappropriate staff behaviour
- + In it's most destructive form, a group of computers controlled by a criminal network called a 'Botnet' can be used to launch a Denial of Service (DoS) attack on a network, flooding it with data, causing down time and disruption. More than 90% of downloads from file sharing clients are unlicensed software. If downloaded using your business Internet Protocol address (IP), the business will be liable to legal prosecution
- + The expense of fixing the problem is likely to far exceed the expense of ensuring preventative measures are in place

Useful Websites

- <http://www.ktn.qinetiq-tim.net/>
- <http://www.berr.gov.uk/whatwedo/sectors/infosec>
- <http://www.bcrc-uk.org>
- <http://www.businesslink.gov.uk>
- <http://www.getsafeonline.org/>
- <http://www.sophos.com/security>
- <http://www.zdnet.co.uk/toolkits/securitythreats>

For more about Botnets

- <http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotnetCharts>

Business Type	Method of Attack	Negative Consequences	Solution	Cost
BASIC + Not linked to the internet + Administration only	N/A	N/A	N/A	N/A
ONLINE COMPUTER USER + Single machine linked to the internet + Receive email/transact online (includes laptops, smart-phones, Blackberrys, PDA's)	+ Opening email attachments + Clicking on hyperlinks in emails + Web-surfing – drive by downloads + File sharing + Using infected audio/video online	+ Loss of computer resources + Loss of productivity + Reputational damage + Source of illegal spam mail-outs + Unwittingly take part in denial of service attacks (DoS) + Risk of virus and spyware attacks	+ Install anti-virus and anti-spyware + Install a personal firewall + Ensure clients and colleagues are aware of infected emails + Limit access to websites except for business use + Install latest web browser + Disable ActiveX and Java scripts	+ Low cost + Medium cost + Low to High cost + No cost + No cost + No cost
NETWORKED + Same as above, but a collection of computers form a network	As above but also: + Via another infected computer on the network	As above but also: + Extreme loss of productivity if all computers are part of a botnet + Risk of becoming victims of a Botnet and DoS which could severely damage business + Risk of infecting clients via mailing lists	Solutions the same as the above but also: + Install a firewall for your server + Disconnect infected machine from network	+ High cost + No cost
ONLINE TRADER + Uses an e-commerce strategy to sell products to a global audience	+ As above	As above but also: + Damage to company reputation and loss of business is likely to be more severe in the event of a DoS attack	Solutions the same as above but also: + Software that provides traffic flow analysis and bandwidth analysis is available	+ High cost – seek professional advice