One is not enough to be “Operation Spam Zombie” ready

Submitted by: Dexterity
Wednesday, 8 June 2005

FAO: NewsDesk

Checkbridge PR Contacts: Jane Lee on jane.lee@dexterity.co.uk t: +44 (0)1273 470199

Liz Merrick on lmerrick@checkbridge.com t: +44 (0)1978 369093
www.checkbridge.com

- Checkbridge study confirms all PC users need multiple email scanners and supports the call for ISPs to provide clean email -

London, 8 June 2005 -- Today, Checkbridge, the managed email filtering service provider, makes public the results of research into viruses caught by three market leading email scanners running on two million emails, over a five day period. This study comes at a time when the US Federal Trade Commission (FTC), in conjunction with the Office of Fair Trading and the London Action Plan (LAP), is demanding that ISPs get tough on spam. The study demonstrates that using just one email scanner for protection is not adequate for businesses or consumers.

The focus of Operation Spam Zombie is on stopping virus’s tapping into people's home computers and using them to send millions of unsolicited spam e-mails. Once these computer have been hijacked by the spammers' software they are known as 'Zombies' and can be used to bombard other consumers with spam e-mails without the computer owners' knowledge. By using this trick the spammers keep their identity secret from the recipients of the spam and from the authorities trying to track them down.

The Checkbridge study highlights that the different filters are individually good in different ways but used alone they are inadequate to stop ‘Zombies’. Each has its own strengths and weaknesses for capturing certain kinds of viruses based on the filtering techniques that it uses (for example, signature-based, heuristic or predictive scanning).

The Checkbridge study analysed two million emails over a five day period. It found that:
§ The email scanners performance varied from 72% to 93.6% stopped across the five days. § No single scanner caught all the viruses. Each scanner caught a number of viruses that were missed by the other two.
§ The performance of each scanner varied on a daily basis. On the worst day the percentage caught by one of the scanners was just 64%.

§ If you relied on the best performing scanner only on each day (which varied) you would have stopped between 89% and 97% of viruses. The best performer however could not be predicted.
§ The number of unique viruses caught varied from 12 per day to 67 per day.

The main victims of Botnets and Zombies are residential subscribers. And although over 50% of consumers and 62% of small to medium sized businesses recognise that multiple scanners are now required (Source: Checkbridge, April 2005), most use single spam and virus scanners based on their PCs. Essentially, those most at risk are least protected.

Checkbridge believes that it is essential to have more than one' signature-based' scanner (to reduce the window of opportunity for getting a virus) plus a heuristic or predictive scanner that is trained to spot as yet unknown viruses. It is only by combining them that you can maximise your protection against Botnets and Zombies and benefit from the strengths of each.

"We fully support the LAP campaign. ISPs are in an ideal place to clean up their customers' email." states John Turley, managing director of Checkbridge. "Getting tough on malware can only be achieved through effective anti-virus and anti-spam defences that identify programs that have infiltrated the unprotected user and proactively identify rogue machines within a network. Only multiple scanning solutions can offer this level of protection.

"For reasons of financial and technical viability scanning should no longer just take place on the desktop. This presents a great opportunity for ISPs to offer multi-filter protection to their users – both business, and critically in the case of Zombies and Botnets, to residential users."

The FTC and LAP are calling for ISPs to stop ignoring the spam relay problem and take immediate action by releasing details about identified Botnets or Zombies on ISP networks. The announcement made in May makes a number of recommendations including investigating when a PC is sending unusual amounts of email; adding rate limiting schemes on relay traffic; and implementing mail diversion (Port 25 blocking) through the ISP as standard.

Checkbridge offers a fully managed 'white label' spam and virus filtering solution for ISPs called Border Scout. It is designed for business and residential user bases - delivering unrivalled protection from Botnets and Zombies. Whether 'switched-on' to deliver a spam and virus free network or sold as additional service the Border Scout service will allow businesses

to be Operation Zombie ready.

About Checkbridge
Checkbridge was set up in 2004 to help mitigate the risk of email failure to businesses in Europe. Checkbridge's aim is simply to 'enable trusted communication'. Checkbridge achieves this by providing a fully managed spam and virus filtering service for ISPs, called Border Scout.

Border Scout is a fully managed, configurable, email filtering service, blocking unwanted email at the Internet level, before it reaches a business or residential network or computer. Border Scout leaves an ISP's client with centralised control and visibility of content filtering, without the hassle day-to-day administration.

The Border Scout service is deployed across multiple servers in three premier European data centres, to ensure that the service is available twenty four hours a day, 365 days a year.
For more…
If you would like further information on Checkbridge or Border Scout our web site is www.checkbridge.com, or you can email info@checkbridge.com or call + 44(0) 845 111 8833.

Checkbridge Ltd - Simply enabling trusted communications

.....
APPENDIX
If the table below is corrupted, please email jane.lee@dexterity.co.uk & it will be sent separately.

Checkbridge virus scanner study summary

The statistics below show the relative performance of three market leading virus scanners over a five day period. During that period two million emails were scanned. One scanner is open source software.

Day 1: Virus total 687
Scanner 1 stopped: 589 missed: 98 unique: 15
Scanner 2 stopped: 613 missed: 74 unique: 67
Scanner 3 stopped: 607 missed: 80 unique: 54

Day 2: Virus total 757
Scanner 1 stopped: 556 missed: 201 unique: 11
Scanner 2 stopped: 696 missed: 61 unique: 42
Scanner 3 stopped: 717 missed: 40 unique: 51

Day 3: Virus total 1144
Scanner 1 stopped: 785 missed: 359 unique: 16
Scanner 2 stopped: 1097 missed: 47 unique: 29
Scanner 3 stopped: 1109 missed: 35 unique: 27

Day 4: Virus total 615
Scanner 1 stopped: 396 missed: 219 unique: 20
Scanner 2 stopped: 502 missed: 113 unique: 32
Scanner 3 stopped: 557 missed: 58 unique: 19

Day 5 Virus total 687
Scanner 1 stopped: 476 missed: 211 unique: 12
Scanner 2 stopped: 629 missed: 58 unique: 15
Scanner 3 stopped: 653 missed: 34 unique: 34

Note: ‘Virus total’ is the total number of viruses, based on the results of the scanners in the study, that were in circulation on each day.