> **"We are delighted with CensorNet Email Security, which has worked exceptionally well. We have received no spam and no junk mail at all. It represents excellent value for money and I have had no hesitation in recommending it to my colleagues in the online IT community."**

Martin Pilkington IT Services Manager

Thumbs down for malicious email viruses

The infection of computers at Thumbs Up (Bury) Ltd with the Zeus Trojan caused a major disruption to the business including downtime of their email. This infection occurred while the company was in the process of swapping their email system from BTpop to Microsoft Exchange to improve productivity. However, even after the implementation of Microsoft Exchange, email-borne viruses continued to disrupt the business until the company signed up to CensorNet's cloud-based Email Security.

Company background

Thumbs Up (Bury) Ltd manufactures and supplies plastic housewares and storage products to major supermarkets, high street retailers, garden centres and online outlets throughout the UK, Ireland and the European Union. Formed in 1978, the company now employs around 250 staff and produces more than 70 million injection moulded items across some 2000 product lines at its production and distribution facility in Bury, Lancashire, UK.

The business effects of a major virus infection

The Trojan.Zbot, also called Zeus, attempts to steal confidential information from the compromised computer. It specifically targets system information, online credentials, and banking details, but can be customised by the criminals to gather any sort of information. Infection by this virus at Thumbs Up caused disruption for around six weeks.

Customer
Thumbs Up (Bury) Ltd.

Industry
Manufacturing

Challenge
Email-borne viruses continued to disrupt the business, even after the implementation of Microsoft Exchange.

Solution
CensorNet Email Security

In addition, about a week after the infection the company's telephone lines were temporarily hijacked by hackers posing as BT engineers, so that if the bank phoned to verify any transactions the calls could be intercepted by the hackers and it would appear that they were speaking to the company. Fortunately the bank had previously experienced this tactic, and supplied the company with a new telephone banking security device until the situation was resolved. Given the timing and the nature of the information that can be gathered by the virus, it is likely that the hackers were using information acquired from the virus.

Antivirus clean-up at Thumbs Up
The company's IT Department has a very proactive approach to anti-virus protection which was regularly upgraded. However Zbot penetrated the endpoint security system in place at the time. All suspected infected devices were removed from the network and several anti-virus tools were tried in order to remove the virus until one was found that detected the virus as soon as it was installed. This removed all versions of the virus as well as other viruses not previously identified, so it was rolled out to all devices on the network.

The clean-up process took around six weeks to complete and was handled directly by the IT Manager. Shortly after the infection issue was resolved, the company completed the implementation of a Microsoft Exchange SMTP server on site, instead of receiving mail via BT Pop3. Unfortunately once this went live email viruses once again began to get through as all incoming and outgoing mail was now being routed through a single IP address with no filters in place. This meant another anti-virus solution needed to be found for their email system.

"I spoke to someone who fully understood my needs, the problems that I faced and was able to answer every single question that I had."

Martin Pilkington IT Services Manager

Cloud email solves the problem

Although there are many antivirus products available in the marketplace, the cost of some can be prohibitive for a business and some can be over complicated when customising. So further internet research was carried out and advice was sought from an online IT community.

For Martin Pilkington, IT Services Manager at Thumbs Up, the comprehensive 'live chat' on the CensorNet website about CensorNet Email Security was absolutely crucial in making the decision to buy. He said: "I spoke to someone who fully understood my needs, the problems that I faced and was able to answer every single question that I had."

CensorNet Email Security

CensorNet Email Security is a cloud-based email security and backup service that scans both inbound and outbound email for viruses, phishing threats, content violations and spam. By doing this in the cloud it removes the processing and bandwidth burden on the local email server and also provides a layer of resilience in case of local mail server failures. Email for the customer's domain(s) is redirected to CensorNet servers before it is delivered to the local email server, such as Microsoft Exchange or Exim.

At the core of CensorNet Email Security is a sophisticated rules engine that allows the IT administrator to customise exactly how email flows in and out of the organisation. The rules engine can inspect all aspects of email, including content, attachments, size, headers, recipients to name but a few and take appropriate action, such as quarantine, re-route, notify, reject and more.

"Our experience of business disruption and the time it took to clean up after a major virus infection is one that we never want to repeat ever again."

Martin Pilkington IT Services Manager

CensorNet Ltd.
Network House, Suite 6.01
Basing View, Basingstoke
RG21 4HG, UK
Phone: +44 (0) 845 230 9590
Email: sales@censornet.com

CensorNet A/S
Park Allé 350 D
2605 Brøndby, DK
Phone: +45 70 22 55 33
Email: sales@censornet.com

CensorNet Inc.
11801 Domain Blvd, 3rd Floor
Austin TX 78758, USA
Phone: +1 888 440 8456
Email: sales@censornet.com