FACT SHEET: DECISION TO IMPOSE FINE ON DOLLARREVENUE
December 2007

DollarRevenue
DollarRevenue was a joint venture involving three Dutch enterprises and their directors. DollarRevenue was active from October 2005 until and including November 2006. The offenders earned a little over EUR 1 million through their illegal activities. OPTA will not release the names of the parties involved, awaiting for the decision in the objection against the publication of the penalty.

Activities
DollarRevenue was responsible for the large-scale installation of unsolicited advertising software (known as adware) and surveillance programs (so-called spyware). A total of 22 million PCs were infected, on average 60,000 per day. DollarRevenue was one of the largest distributors of unsolicited software in the world (see www.sunbelt-software.com, the website of a manufacture of anti-spyware software).

Effects
The PCs became virtually unusable due to an avalanche of advertising material. Those PCs which were infected with DollarRevenue's software, were constantly inundated with popup windows containing advertisements. In addition, all sorts of advertising software was installed, such as additional search toolbars, their default home page was changed, and the software communicated details of the PC users' surfing patterns to DollarRevenue.

DollarRevenue's methods
DollarRevenue's software was distributed from servers located in the Netherlands. This occurred in four different ways. For instance, Internet users were first tricked with the aid of misleading or apparently innocent file names. For instance, they were led to believe that they were about to download a video clip, whereas DollarRevenue's software was actually installed on their PCs. Secondly, DollarRevenue disseminated its software using botnets: networks of infected PCs which were controlled by a hacker. Thirdly, it used security loopholes in software ('exploits'). Finally, although information was displayed to end users in a number of cases before any software was installed (using ActiveX), it was inaccurate and incomplete, with the result that Internet users did not know what to expect.

The investigation also revealed that it was impossible or difficult for Internet users to prevent installation or to remove the software. It did not contain an uninstall function and could only be removed with expert assistance.

Network of affiliates

The offenders had a network of intermediaries, also known as affiliates. The latter were other parties who distributed the software further using the above-mentioned methods on DollarRevenue's instructions and in return for a fee.

Investigation

Based on tips and *ex officio* monitoring, regulatory officials within OPTA's Internet Safety Team launched an investigation into DollarRevenue in 2006. Unannounced inspections were conducted in various locations in November 2006. As part of this process regulatory officials gained access to business administration records and computer systems. In addition, various people involved made statements. A report was drawn up based on the findings of these investigations. The relevant companies and their directors were able to present their case in response in both verbal and written form.

Deliberate contraventions

In the course of its investigations OPTA established that the offenders were well aware that they were contravening the law. This was evident in their business plan, amongst other things. In addition, they sought contact with foreign criminal botnet administrators, instructed their affiliates to provide Internet users with incomplete information or none at all, used pseudonyms, developed software of such a nature that it circumvented spyware filters and, for example, ignored complaints which they received from advertisers about their methods.

Regulations

Section 1.4 of the Universal Service and End Users Decree [*Besluit universele dienstverlening en eindgebruikers*], which is based on the Telecommunications Act [*Telecommunicatiewet*], stipulates that users of Internet services must be clearly and accurately informed beforehand of the purposes of any software which is to be installed. Furthermore, a clearly discernible method must be presented to refuse or reverse installation. These businesses failed to comply with these provisions.

Sanctions

Fines totalling EUR 1 million have been imposed for these offences having regard to the gravity and duration of the offences, the culpability of the offenders and the gains they achieved through their offences. Two companies were jointly fined EUR 300,000. The responsible director was also fined with EUR 300,000.00. The other company was fined with EUR 200,000.00, as well as the director. The maximum fine which OPTA can impose for these types of offences on the basis of its policy rules on fines amounts to EUR 300,000.00.

In addition to these fines, this summer a conditional penalty was also imposed on the directors (see OPTA's press release of 15 August 2007). Based on this they are prohibited from the further distribution of unsolicited software.

Also due to the information OPTA obtained from this investigation one of the botnetherders, who was living in New Zealand, is recently arrested by the New Zealand police.

GLOSSARY ACCOMPANYING THE DECISION TO IMPOSE A FINE ON DOLLAREVENUE
November 2007

Malware, spyware, adware
Adware is software which ensures that a computer user gets to see specific advertising materials. Spyware is software which ensures that specific information about a computer user (for example, which website he visits or passwords that he uses) is communicated to some other party. Malware is a collective term for all types of undesirable, malicious software.

Botnet
A botnet is a network of hacked computers (also known as zombies) which can be controlled from remote computers on the Internet without the owner being aware of this.

Botnet herder
A botnet herder is someone who controls a botnet and is capable of issuing instructions to computers which are linked to a botnet. For example, an instruction may be to download software and to install it without the relevant computer owner being aware of this.

Affiliation
Affiliation is a form of business agreement entered into on the Internet. An affiliate may be someone who is connected with an advertising software company. The affiliate and the company enter into an agreement and the affiliate is paid for the installation of that company's advertising software. A unique affiliate code is transmitted in the case of each installation, so that the company knows to whom it owes a fee.

Exploits
Exploits are so-called loopholes in computer programs. Using these loopholes someone may place data on a computer without its owner's consent.

ActiveX
ActiveX is a method of exchanging files between a website and a computer belonging to a user or subscriber. ActiveX technology has been developed by Microsoft to allow software applications to be installed via the Internet.