



Kaspersky Lab helps Dutch police dismantle Shadow botnet

The Dutch High Tech Crime Unit identified a large botnet when they arrested a 19 year old Dutch man last week. The Unit asked Kaspersky Lab, a leading developer of secure content management solutions, to provide the victims with instructions on how to neutralize the malware on their systems; neutralizing the malware ultimately brings down the botnet. This is an excellent example of the close co-operation which exists between the antivirus industry and law enforcement.

At the request of the Dutch police, Kaspersky Lab created detailed instructions on how to remove the malware. The Dutch police have pointed victims towards a page on the Kaspersky Lab website which contains the removal instructions, and also to a website which gives victims the opportunity to make a formal complaint to the police. Eddy Willems, Security Evangelist with Kaspersky Lab Benelux, who worked closely with the High Tech Crime Unit, believes this case clearly illustrates how the security industry can help law enforcement in the fight against cybercrime. A spokesperson for the Public Prosecution Service agrees: "The Public Prosecution Service and the police worked together with Kaspersky Lab on this case with full contentment".

The so-called Shadow botnet is made up of around 100,000 infected machines from all over the world. A botnet is a collection of computers infected with malware which are then linked into a network. The infected machines can be controlled remotely (without their owners' knowledge or consent) and used by criminals to send spam, attack websites, or steal confidential data such as credit card numbers.

Last week the Dutch police arrested a 19 year old Dutch man for selling this botnet to a Brazilian who was also arrested. The arrests were the result of an operation conducted by the High Tech Crime Unit and the FBI.

If you think you're a victim

If you think your computer is part of the botnet, please follow the removal instructions at www.kaspersky.com/shadowbot. However, the removal instructions only apply to the malware which has been used to create the botnet. Eddy Willems warns: "These programs may have downloaded additional malware to computers which were part of the botnet. So users should make sure they perform a full scan of their machine using an up-to-date antivirus solution." If you have Kaspersky® Internet Security or Kaspersky® Anti-Virus running on your computer, you do not need to follow the instructions, as the software will automatically detect and delete the malware.