



## Symantec Threat Bulletin: Mariposa Botnet Arrests

It is being reported that Spanish authorities have arrested three individuals allegedly associated with the operation of what has been dubbed the Mariposa Botnet. The botnet, like most, was used to steal personal information that criminals could use for financial gain, such as credit card numbers. Cybercrime represents today's most prolific threat and cybercriminals are more determined than ever to steal confidential information. They are continuing their shift away from noisy, large-scaled attacks to highly targeted silent attacks motivated by financial gain. They can be commercial entities breaking into competitors records, or international crime rings stealing valuable data like credit card numbers and email passwords.

In 2009, 90 percent of threats observed by Symantec were targeting confidential information. We released the results of our 2010 Enterprise security study last week, which surveyed 2,100 enterprise CIOs, CISOs and IT managers around the world and our study showed that 75 percent of enterprises experienced cyber attacks.

Symantec has observed that the majority of today's malware contains a bot command and control channel. Botnets are in essence a large collection of malware-infected computers under the control of a central bot master, the cybercriminal or cybercrime groups that "owns" the botnet. They are used for a myriad of purposes, from sending spam to conducting denial of service-type attacks or stealing information.

There's also been a marked increase in crimeware, or software used to conduct cybercrime. These tools fuel the black market including, botnets, keystroke loggers, spyware, backdoors, and Trojans. User-friendly toolkits such as Zeus enable even novice hackers to create malware and botnets. In the case of the Mariposa Botnet, Symantec believes the network of infected computers stemmed in large part from the Butterfly toolkit, which is actually no longer for sale on the underground economy. Detection names of the malware associated with the Butterfly toolkit vary, but Symantec detects the threat as W32.Pilleuz. Here's a brief rundown of what the threat does:

It spreads through file-sharing programs, Microsoft instant messaging clients, and removable drives.

It opens a back door on the compromised computer, essentially giving a remote attacker full control over the compromised computer.

It uses a variety of packing techniques.

It communicates with remote servers at the following network addresses:- `qwertasdfg.sinip.es`- `butterfly.sinip.es`- `bfisback.no-ip.org`

In 2009, Symantec created over 2.9 million new virus signatures and discovered more than 211 million distinct malware variants. To put this in perspective we've created more signatures in the past 15 months than in the past 18 years combined. Last year Symantec launched its new reputation-based security, which was built to address the untold number of undetected threats created every day. This technology leverages the wisdom of tens of millions of Symantec users around the world to derive safety ratings for every file on the Internet. It allows Symantec Security Response experts to compute the reputation of a program based on a number of different factors including the origin, the age of the program and its prevalence. In just six months Symantec has generated more than 177 billion reputation ratings.

For a more comprehensive description of this threat, please visit this posting on Symantec's Security Response blog.

Do let us know if you would like to speak to one of our security experts about how fake antivirus software works and what can be done to avoid falling victim to these scams. Media Contact: Jasmin Athwal Max Australia +61 2 9954 3492 [Jasmin.Athwal@maxaustralia.com.au](mailto:Jasmin.Athwal@maxaustralia.com.au)