

Panda Security and Defence Intelligence Coordinate Massive Botnet Shutdown with International Law Enforcement

- Collaborative cybercrime investigation results in three arrests, more pending
- Personal and financial data compromised from massive cyber attack impacting nearly 13 million unique IP addresses, 50 percent of Fortune 1000 companies
- Preliminary damages estimated to be in the millions of dollars

RSA CONFERENCE 2010, SAN FRANCISCO, Mar. 3, 2010 – According to IT security firms [Defence Intelligence](#) and [Panda Security](#), the Mariposa botnet, a massive network of infected computers designed to steal sensitive information, has been shutdown and three suspected criminals accused of operating the botnet have been arrested by Spanish law enforcement. Mariposa stole account information for social media sites and other online email services, usernames and passwords, banking credentials, and credit card data through infiltrating an estimated 12.7 million compromised personal, corporate, government and university IP addresses in more than 190 countries. The botnet was shutdown and rendered inactive on December 23rd, 2009 thanks to the collaborative effort of different security experts and law enforcement, including Panda Security, Defence Intelligence, the FBI and Spanish Guardia Civil.

With almost 13 million compromised computers, Mariposa is one of the largest botnets ever reported on record. Christopher Davis, CEO for Defence Intelligence, who first discovered the Mariposa botnet, explains: "It would be easier for me to provide a list of the *Fortune* 1000 companies that weren't compromised, rather than the long list of those who were."

Following the discovery of Mariposa's existence in May 2009, Defence Intelligence, Panda Security and the Georgia Tech Information Security Center spearheaded the Mariposa Working Group as a collaborative effort with other international security experts and law enforcement agencies to eradicate the botnet and bring the perpetrators to justice. The main botmaster, nicknamed "Netkairo" and "hamlet1917", as well as his immediate botnet operator partners, "Ostiator" and "Johnyloleante", were arrested earlier this month.

Pedro Bustamante, senior research advisor at Panda Security, said: "Our preliminary analysis indicates that the botmasters did not have advanced hacking skills. This is very alarming because it proves how sophisticated and effective malware distribution software has become, empowering relatively unskilled cyber criminals to inflict major damage and financial loss. We're extremely proud of the coordinated effort made by all of the Mariposa Working Group members and the speed at which we were able to bring down this massive botnet and the criminals behind it."

Late last year, the Mariposa Working Group infiltrated the command-and-control structure of Mariposa to observe the communication channels used by the suspected botmasters. These channels relay information from the compromised computers to the perpetrators and are commonplace, similar to those used by the Zeus, Conficker and Koobface botnets or as shown recently in the Google/Aurora operation. After analyzing the main command-and-control servers the Working Group was able to facilitate the coordinated worldwide shutdown of the Mariposa Botnet on December 23rd. Panda Security is currently

leading a comprehensive analysis of the malware, as well as coordinating international communication among other antivirus companies to ensure that their signatures are updated. Highlights from Panda Security's preliminary analysis include:

- Once infected by the Mariposa bot client, the botmaster installed different malware (advanced keyloggers, banking trojans like Zeus, remote access trojans, etc.) in order to gain additional functionality into the zombie PCs.
- The botmaster made money by selling parts of the botnet, installing pay-per-install toolbars, selling stolen credentials for online services and using the stolen banking credentials and credit cards to make transactions to overseas mules.
- The Mariposa botnet spread extremely effectively via P2P networks, USB drives, and MSN links.

A more comprehensive report from Panda Security's forensic analysis will be available at <http://pandalabs.pandasecurity.com> shortly. In the meantime a short description of the Mariposa botnet software can be found at <http://www.pandasecurity.com/homeusers/security-info/217587/ButterflyBot.A>.

"Once again, the coordinated efforts of various international law enforcement agencies and Spain's Guardia Civil, together with the Internet security industry, have been able to tackle the global threat of cyber-crime," said Juan Salom, commander of the Cybercrime Unit of the Guardia Civil.

According to Dave Dagon at the Georgia Tech Information Security Center: "Instead of making pie charts, we should treat a botnet as a crime scene and not just a research project."

The Mariposa Working Group has officially seized control of the communication channels used by Mariposa, effectively severing the botnet from its criminal creators. In an apparent act of retaliation, a Distributed Denial of Service (DDoS) attack was initiated against Defence Intelligence shortly after the botnet was shut down in December. The attack was powerful enough to impact one large Internet Service Provider, many of whose customers were knocked offline for several hours.

According to a representative from CDmon, the ISP that collaborated in the investigation and where the criminal domains were hosted: "We are pleased to have been able to support this international operation, along with the Spanish Guardia Civil, Panda Security, Defence Intelligence and other law enforcement agencies, and to help bring down the botnet. CDmon is strongly committed to the concept of quality Internet, guaranteeing standards of quality and security across all our services. This collaborative effort is a big win in the fight against cybercrime."

"We will continue to fight the threat of botnets and the criminals behind them," says Davis. "We'll start by dismantling their infrastructure and won't stop until they're standing in front of a judge."

Defence Intelligence and Panda Security are attempting to contact affected organizations. To find out if your organization has been compromised, contact compromise@defintel.com or info@pandasecurity.com.

About Defence Intelligence:

Defence Intelligence is a privately held information security firm specializing in compromise protection. Based in Ottawa, Canada, the founders of Defence Intelligence are globally recognized industry experts. They have headed information security for Fortune 50 companies, consulted with hundreds of private enterprises and government agencies, and have assisted in the capture and prosecution of international computer criminals. For more information, visit <http://www.defintel.com>.

About The Guardia Civil

The Guardia Civil is one of two national police forces in Spain and its missions include ensuring public security, administrative policing, customs and revenue, intelligence services and the Central Operative

Unit, a branch of the Judicial Police responsible, among other things, for the fight against organized crime
For more information at: <http://www.guardiacivil.org/index.jsp>

About Panda Security

Founded in 1990, Panda Security is the world's leading provider of cloud-based security solutions, with products available in more than 23 languages and millions of users located in 195 countries around the world. Panda Security was the first IT security company to harness the power of cloud computing with its Collective Intelligence technology. This innovative security model can automatically analyze and classify thousands of new malware samples every day, guaranteeing corporate customers and home users the most effective protection against Internet threats with minimum impact on system performance. Panda Security has 56 offices throughout the globe with US headquarters in California and European headquarters in Spain.

Panda Security collaborates with Special Olympics, WWF and Invest for Children as part of its Corporate Social Responsibility policy.

For more information, visit <http://www.pandasecurity.com/>.

For more information:

comunicacion@pandasecurity.com

Tel. +34 91 806 37 00