



Australian Government

Attorney-General's Department



AUSTRALIA'S NATIONAL  
COMPUTER EMERGENCY RESPONSE TEAM

# CERT Australia Industry News

## Arrests made in relation to the Mariposa Botnet.

The FBI has recently published a press release [1] relating to the arrest of the creator and a number of operators of the Mariposa Botnet through a joint operation by the FBI, the Slovenian Criminal Police and the Spanish Civil Guard.

### Technical Details

The Botnet which reportedly controlled as many as 8-12 million computers was used to capture banking credentials, spread malware and conduct Denial of Service attacks. The botnet grew to such a size through the distribution of malware such as Rimecud [2]. Mariposa was also reportedly spreading malware via Vodafone HTC Magic mobiles [3] back in March of this year. Whilst not infecting the phone itself, it would spread once the phone was connected to a Windows computer via USB.

### Business Impact

If the command and control server has been disabled as a result of this investigation, it would mean the infected machines would no longer be able to receive commands and report back. However the machines would remain infected and may be taken over by another controller due to the functionality of the malware used. These infected machines would then continue to send compromise credentials and take part in attacks against other systems.

### Further Reading

- [1] <http://fbi.gov/pressrel/pressrel10/mariposa072810.htm>
- [2] <http://blogs.technet.com/b/mmpc/archive/2010/03/04/in-focus-mariposa-botnet.aspx>
- [3] <http://www.zdnet.com/blog/security/vodafone-htc-magic-shipped-with-conficker-mariposa-malware/5626>

This document remains the property of the Australian Government. The information contained in this document is for the use of the intended recipient only and may contain confidential or privileged information. If this document has been received in error, that error does not constitute a waiver of any confidentiality, privilege or copyright in respect of this document or the information it contains. This document and the information contained herein cannot be disclosed, disseminated or reproduced in any manner whatsoever without prior written permission from the Assistant Secretary, E-Security Policy and Coordination, Attorney-General's Department, 3 - 5 National Circuit, Barton ACT 2600.

The material and information in this document is general information only and is not intended to be advice. The material and information is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. You should base any action you take exclusively on your own methodologies, assessments and judgement, after seeking specific advice from such relevant experts and advisers as you consider necessary or desirable. **To the extent permitted by law, the Australian Government has no liability to you in respect of damage that you might suffer that is directly or indirectly related to this document, no matter how arising (including as a result of negligence).**