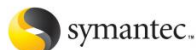


14 December 2006

By: Marius Oiaga, Technology News Editor

[The Coordinates of an MS Word Attack](#)

Vulnerability, Exploit and Attack



The Cupertino-based security outfit Symantec revealed that the analysis of Bloodhound.Exploit.106 samples returned as a result of a heuristic method released for the zero-day Word vulnerability (Microsoft Security Advisory 929433) resulted in the identification of a maliciously crafted Word document. "We found a malicious Word document that was written in Portuguese and added detection for it as Trojan.Mdropper.T. The document contains an exploit that drops an executable file, which then installs a downloader threat and opens a clean Word document in an Asian language with some strange predictions about the future. The downloader then downloads a keylogger/infostealer. Detections for all of this malicious code are included in today's certified definitions," explained Amado Hidalgo, Symantec Sr. Security Response Manager. Symantec additionally detected a copy of the original Portuguese document designed to be compatible with a free word processing application. Both documents are malformed and will crash MS Word, but the latter will also conduct to remote code execution. "The original document is publicly available on a number of Web sites, so we suspect the malicious code writers may have stumbled upon it and used it as a "template", transforming an innocent bug into a working exploit. In fact, the final malicious Word file contains an encrypted shellcode (probably generated using the Metasploit suite) and a malicious executable file," added Hidalgo.