Trojan.Win32.Sofacy.A

TSL ID	TSL20110908-01
Severity	Moderate
Description	Trojan.Win32.Sofacy.A is a Trojan that targets the Windows platform. This malware communicates to a remote server, acknowledging the infection as well as sending and receiving other status messages. In addition, it targets various applications for stealing user credentials, such as, The Bat!, Qualcomm Eudora, Mozilla Firefox, Internet Explorer and others. Moreover, the malware encrypts the collected data and send them to a predefined list of email addresses. The malware arrives on target systems via a specially crafted Microsoft Office Word document that exploits one of the following vulnerabilities: CVE-2009-3129, CVE-2010-3333.
Affected Products	• Microsoft Windows All Versions
File Hashes	MD5: • 1E217668D89B480AD42E230E8C2C4D97 • 9E4817F7BF36A61B363E0911CC0F08B9 • E1554B931AFFB3CD2EDC90BC58028078 • ED7F6260DEC470E81DAFB0E63BAFB5AE SHA1: • AC6B465A13370F87CF57929B7CFD1E45C3694585 • C01B02CCC86ACBD9B266B09D2B693CB39A2C6809
Identifiers	Microsoft Malware Protection Center: PWS:WIN32/SUKWIDON.A, TROJAN:WIN32/SEDNIT.B Symantec: INFOSTEALER.SOFACY TrendMicro: BKDR_SEDNIT.AE, TROJ_DROPPR.ZCV ESET: WIN32/PSW.AGENT.DVDXCIK Jiangmin: TROJAN/VILSEL.OQY
References	http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3AWin32%2FSukwidon.A http://www.symantec.com/business/security_response/writeup.jsp?docid=2011-090714-2907-99&tabid=2
Related Threats	TSL20150713-04 - Trojan-Downloader.Win32.Sofacy.B TSL20141028-04 - Trojan-Downloader.Win32.Coreshell.A TSL20101109-13 - Microsoft Office RTF Stack Buffer Overflow TSL20091110-07 - Microsoft Office Excel Featheader Record Memory Corruption