(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 October 2002 (10.10.2002)

PCT

(10) International Publication Number
WO 02/079956 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/09414

(22) International Filing Date: 26 March 2002 (26.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/823,673 30 March 2001 (30.03.2001) US

(71) Applicant: COMPUTER ASSOCIATES THINK, INC. [US/US]; One Computer Associates Plaza, Islandia, NY 11749 (US).

(72) Inventors: MALIVANCHUK, Taras; Zalman Aran 24/5 St., Holon (IL). DARZI, Moshe; Gutman 14 St., Petach Tikva (IL). ROTSCHIELD, Ofer; Yigal Alon 7 St., Kiryat Uno (IL).

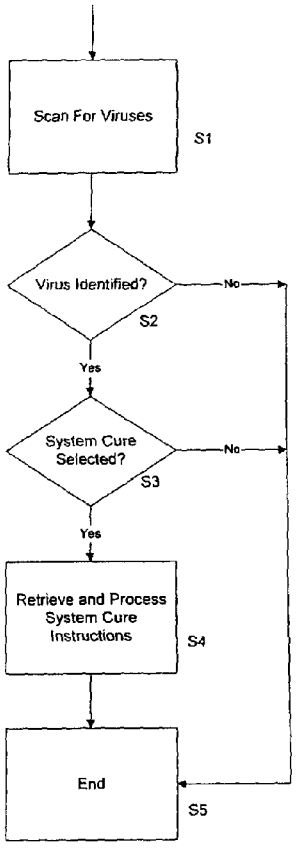
(74) Agent: JAWORSKI, Richard, F.; Cooper & Dunham LLP, 1185 Avenue of the Americas, New York, NY 10036 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR RESTORING COMPUTER SYSTEMS DAMAGED BY A MALICIOUS COMPUTER PROGRAM



(57) Abstract: A method for restoring a computer system modified by malicious code. The method scans the computer system for the malicious code, identifies the malicious code and retrieves from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code. The at least one command is executed to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

WO 02/079956 A1

GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:
— *with international search report*