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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2002 (24.01.2002)

PCT

(10) International Publication Number
WO 02/006928 A3

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

(21) International Application Number: PCT/US01/19142

(22) International Filing Date: 14 June 2001 (14.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/218,489 14 July 2000 (14.07.2000) US
09/642,625 18 August 2000 (18.08.2000) US

(71) Applicant: VCIS, INC. [US/US]; 522 Erskine Drive, Pacific Palisades, CA 90272 (US).

(72) Inventor: VAN DER MADE, Peter, A., J.; 17 Nooal Street, Newport Beach, NSW 2106 (AU).

(74) Agents: WRIGHT, William, H. et al.; Hogan & Hartson L.L.P., Biltmore Tower, Suite 1900, 500 South Grand Avenue, Los Angeles, CA 90071 (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, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

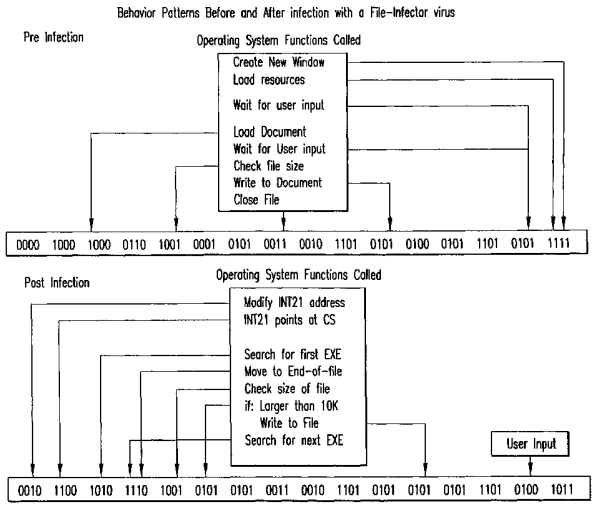
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
14 August 2003

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.

(54) Title: COMPUTER IMMUNE SYSTEM AND METHOD FOR DETECTING UNWANTED CODE IN A COMPUTER SYSTEM



(57) Abstract: An automated analysis system detects malicious code within a computer system by generating and subsequently analyzing a behavior pattern for each computer program introduced to the computer system. Generation of the behavior pattern is accomplished by a virtual machine invoked within the computer system. An initial analysis may be performed on the behaviour pattern to identify infected programs on initial presentation of the program to the computer system. The analysis system also stores behavior patterns and sequences with their corresponding analysis results in a database. Newly infected programs can be detected by analyzing a newly generated behaviour pattern for the program within reference to a stored behavior pattern to identify presence of an infection or payload pattern.

WO 02/006928 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/19142

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

INSPEC, EPO-Internal, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JIEH-SHENG LEE ET AL: "A generic virus detection agent on the Internet" SYSTEM SCIENCES, 1997, PROCEEDINGS OF THE THIRTIETH HWAII INTERNATIONAL CONFERENCE ON WAILEA, HI, USA 7-10 JAN. 1997, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 7 January 1997 (1997-01-07), pages 210-219, XP010271868 ISBN: 0-8186-7743-0	1,2,4,5, 10
A	page 210, left-hand column, line 1 -page 211, left-hand column, paragraph 4 page 213, right-hand column, last paragraph -page 214, right-hand column, line 24 page 215, paragraphs D,E	11,17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 2003	17/01/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/19142

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 636 977 A (CHAMBERS DAVID ALAN) 1 February 1995 (1995-02-01)	1
A	abstract column 4, line 21 - line 51 column 8, line 31 - line 40 column 9, line 11 -column 11, line 14 column 12, line 13 - line 44	2,4,11
X	WO 99 15966 A (SYMANTEC CORP) 1 April 1999 (1999-04-01)	11
A	abstract page 9, line 9 - line 21 page 13, line 3 - line 7 page 14, line 11 - line 13 page 22, line 20 - line 26	1
A	US 5 842 002 A (KLEMMER TIMOTHY J ET AL) 24 November 1998 (1998-11-24) abstract column 8, line 27 - line 35	1,11
A	US 5 854 916 A (NACHENBERG CAREY S) 29 December 1998 (1998-12-29) abstract column 4, line 40 -column 5, line 4 column 6, line 6 - line 58	1,6-8, 11,13-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/19142

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0636977 A	01-02-1995	US 5398196 A	14-03-1995
		DE 69427252 D1	28-06-2001
		DE 69427252 T2	03-01-2002
		EP 0636977 A2	01-02-1995
WO 9915966 A	01-04-1999	US 6357008 B1	12-03-2002
		CA 2304163 A1	01-04-1999
		DE 69802831 D1	17-01-2002
		DE 69802831 T2	25-04-2002
		EP 1018077 A1	12-07-2000
		WO 9915966 A1	01-04-1999
US 5842002 A	24-11-1998	AT 183592 T	15-09-1999
		CA 2191205 A1	07-12-1995
		DE 69511556 D1	23-09-1999
		EP 0769170 A1	23-04-1997
		JP 10501354 T	03-02-1998
		WO 9533237 A1	07-12-1995
US 5854916 A	29-12-1998	US 5765030 A	09-06-1998
		US 6067410 A	23-05-2000
		US 5696822 A	09-12-1997
		DE 69712635 D1	20-06-2002
		EP 0941512 A1	15-09-1999
		WO 9824023 A1	04-06-1998
		US 5999723 A	07-12-1999
		WO 9803916 A1	29-01-1998
		AU 1848597 A	28-08-1997
		CA 2244892 A1	14-08-1997
		DE 69702335 D1	27-07-2000
		DE 69702335 T2	30-11-2000
		EP 0880743 A2	02-12-1998
		WO 9729425 A2	14-08-1997
		AU 7247796 A	17-04-1997
		DE 69609980 D1	28-09-2000
		DE 69609980 T2	08-02-2001
		EP 0852763 A1	15-07-1998
		WO 9712322 A1	03-04-1997
		US 5826013 A	20-10-1998