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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2012 (06.12.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/167056 A3

(51) International Patent Classification:
G06F 21/00 (2013.01) *G06F 11/30* (2006.01)

(21) International Application Number:
PCT/US20 12/040428

(22) International Filing Date:
1 June 2012 (01 .06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/15 1,173 1 June 201 1 (01 .06.201 1) US

(71) Applicant *(for all designated States except US):* **MCAFEE, INC.** [US/US]; 3965 Freedom Circle, Santa Clara, CA 95054 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only):* **AGARWAL, Romanch** [IN/IN]; #67/2, Wazir Hasan Road, Lucknow 226001 (IN). **SINGH, Prabhat Kumar** [IN/IN]; #001, Skylark Enclv, 5th Main, New Thippasandra, Bangalore 560102 (IN). **JYOTI, Nitin** [IN/IN]; #605, Block 20, Sun City Apts., Bangalore 560102 (IN). **VISHWANATH, Harinath Ramachetty** [IN/IN]; #25/2, 4th Main, M.S. Ramaiah City, J.P. Nagar, 8th Phase, Bangalore 560076 (IN). **PRASHANTH, Palasamudram Ramagopal** [IN/IN]; #83, Flat-Fl, Laxmipriya Residency, 2nd Cross, K.V. Layout, 4th Block East, Jayanagar, Bangalore 56001 1 (IN).

(74) Agent: **SUVA II, Jerry, F.;** Baker Botts L.L.P., 98 San Jacinto Blvd., Suite 1500, Austin, TX 78701 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR NON-SIGNATURE BASED DETECTION OF MALICIOUS PROCESSES

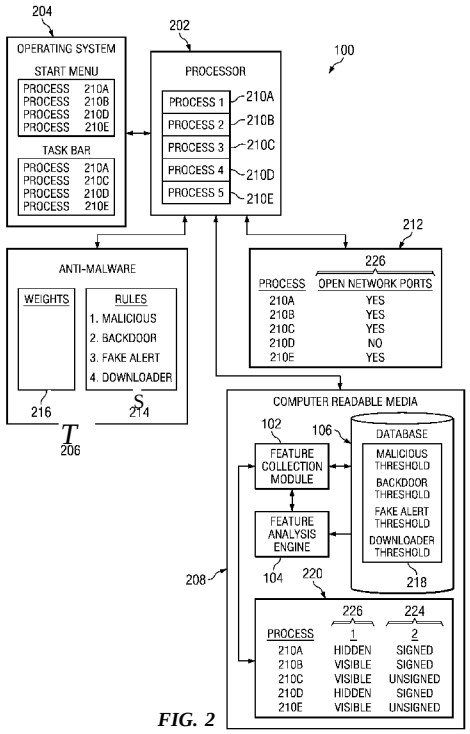

FIG. 2

(57) Abstract: Systems and methods for detecting malicious processes in a non-signature based manner are disclosed. The system and method may include gathering features of processes running on an electronic device, applying a set of rules to the features, and applying a statistical analysis to the results of the rules application to determine whether a process should be classified into one or more of a plurality of process categories.

WO 2012/167056 A3

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(H))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:

2 8 February 201 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/040428

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00(2006.01)i, G06F 11/30(2006.01)i

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)

G06F 21/00; G06F 11/30; H04L 9/00; G06F 15/18; G06F 11/00

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: score, compare, threshold, classify, malicious, program

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004-0054917 A1 (MARK 0BRECHT et al.) 18 March 2004	1,3-11,13-20
A	See the abstract; paragraphs 16-30; claims 1,8; and figure 2.	2,12
A	US 2010-0153316 A1 (DUFFIELD NICHOLAS et al.) 17 June 2010 See the abstract; paragraphs 10-19; claim 1; and figure 2.	1-20
A	US 2005-0283837 A1 (MICHAEL OLIVIER et al.) 22 December 2005 See the abstract; paragraphs 112-130; and figures 1-5.	1-20
A	US 2008-0016339 A1 (JAYANT SHUKLA) 17 January 2008 See the abstract; paragraphs 121-132; and figures 1-12.	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family 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 application or patent 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 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
20 DECEMBER 2012 (20.12.2012)	**20 DECEMBER 2012 (20.12.2012)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Soak, Sang Moon Telephone No. 82-42-481-8470

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2012/040428

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004-0054917 A1	18.03.2004	AU 2003-265813 A1	19.03.2004
		EP 1546891 A1	29.06.2005
		EP 1546891 A4	05.09.2007
		EP 1590723 A2	02.11.2005
		EP 1590723 A3	16.11.2005
		US 2004-0064736 A1	01.04.2004
		US 2004-0098607 A1	20.05.2004
		US 2004-0187023 A1	23.09.2004
		US 2008-0209561 A1	28.08.2008
		US 2010-0095379 A1	15.04.2010
		US 7331062 B2	12.02.2008
		US 7509679 B2	24.03.2009
		US 7748039 B2	29.06.2010
		US 7832011 B2	09.11.2010
		US 7930751 B2	19.04.2011
		US 8156552 B2	10.04.2012
		WO 2004-021197 A1	11.03.2004
		WO 2004-072777 A2	26.08.2004
		WO 2004-072777 A3	26.08.2004
US 2010-0153316 A1	17.06.2010	None	
US 2005-0283837 A1	22.12.2005	US 7748038 B2	29.06.2010
		WO 2006-009620 A1	26.01.2006
US 2008-0016339 A1	17.01.2008	None	