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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number
WO 2004/088483 A2

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

(21) International Application Number:
PCT/GB2004/000214

(22) International Filing Date: 19 January 2004 (19.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0307736.9 3 April 2003 (03.04.2003) GB

(71) Applicant *(for all designated States except US)*: **MESSAGELABS LIMITED** [GB/GB]; 1270 Landsdowne Court, Gloucester Business Park, Gloucester GL3 4AB (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SHIPP, Alexander** [GB/GB]; Star Internet, Brighouse Court, Barmwood, Gloucester GL4 3RT (GB).

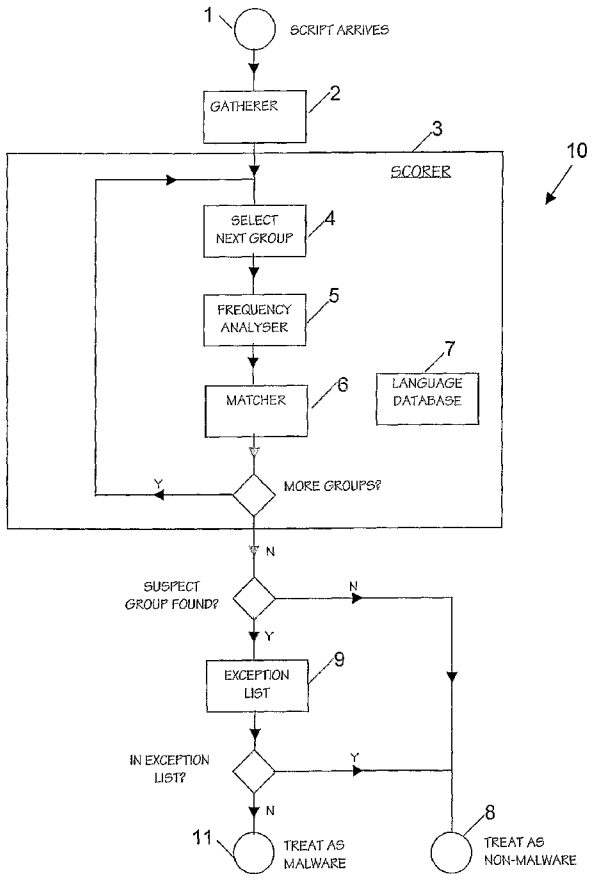
(74) Agents: **AYERS, Martyn, Lewis, Stanley** et al.; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: SYSTEM FOR AND METHOD OF DETECTING MALWARE IN MACROS AND EXECUTABLE SCRIPTS



(57) Abstract: An anti malware scanner for files is provided with means for processing script and macro files and flagging them as suspect or not based upon an automated analysis of source code in the file. This analysis involves separating the program source into groups of parts such as comment, variable names and routine names, eliminating duplicates and performing a character frequency distribution analysis of the resulting strings. The system may include an exception list to omit flagging a file as suspect if it is on the exception list.

WO 2004/088483 A2

Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

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.