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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 April 2006 (13.04.2006)

PCT

(10) International Publication Number
WO 2006/039352 A3

(51) International Patent Classification:
G06F 11/30 (2006.01)

(21) International Application Number:
PCT/US2005/034874

(22) International Filing Date:
28 September 2005 (28.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/956,573	1 October 2004 (01.10.2004)	US
10/956,578	1 October 2004 (01.10.2004)	US
10/956,574	1 October 2004 (01.10.2004)	US

(71) Applicant *(for all designated States except US)*: **WEBROOT SOFTWARE, INC.** [US/US]; 2560 55th Street, Boulder, CO 80301 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **THOMAS, Steve** [US/US]; 2420 Panorama Ave., Boulder, CO 80304 (US). **GREENE, Michael, P.** [US/US]; 1760 Linden Avenue, Boulder, CO 80304 (US). **STOWERS, Bradley, D.** [US/US]; 2558 Jarett Drive, Mead, CO 80542 (US). **BARTON, Kevin** [US/US]; 10253 Robb Street, Broomfield, CO 80021 (US). **HERMAN, Jeffery** [US/US]; 5646 Rim Rock Court, Boulder, CO 80301 (US).

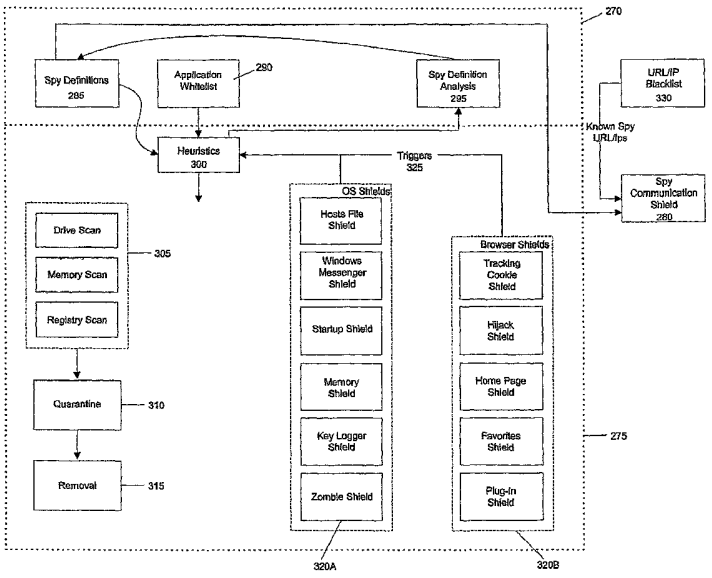
(74) Agents: **GALLIANI, William, S.** et al.; Cooley Godward, LLP, One Freedom Square, Reston Town Center, Reston, VA 20190-5601 (US).

(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, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 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, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PESTWARE DETECTION



(57) Abstract: Methods for monitoring network communications between a protected computer and a remotely-located computer such as a Web server are described. One embodiment is configured to intercept a data packet transmitted from a protected computer. This embodiment then compares the destination address of the data packet against a list of approved destination addresses. When the destination address is included in the list of approved destination addresses, then the packet is delivered to the destination address. If the packet is not addressed to an approved address, then it is evaluated for pestware traces. Embodiments of the invention can also be configured to monitor incoming traffic to a protected computer.

WO 2006/039352 A3

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(88) Date of publication of the international search report:
31 August 2006

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/34874

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 11/30 (2006.01)
USPC - 726/22
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)
U.S. : 726/11,13,22 713/ 188, 154, 152, 165

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PUBWEST --PGPB, USPT, EPAB, and JPAB--searched spyware, malware, pestware, adware, malicious, quarantine, detect, find, firewall, compare, registry, scan, packet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/0034794 A1 (MAYER et al.) 19 February 2004 (19.02.2004) see claim 2, 3, 4, and paragraphs 108, 115, 119, 127, and 128	1-17
A	US 2004/0187023 A1 (ALAGNA et al.) 23 September 2004 (23.09.2004) see claim 5 and 6 and paragraphs 53,58, 75, 64, 93, 94, and 97	1-32
A	US 6,633,835 B1 (MORAN et al.) 14 October 2003 (14.10.2003) see entire document	1-32
A	US 2004/0143763 A1 (RADATTI) 22 July 2004 (22.07.2004) see entire document	1-32

☐ 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 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
03 March 2006 (03.03.2006)	05 JUL 2006
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver Telephone No. 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)