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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 August 2006 (31.08.2006)

PCT

(10) International Publication Number
WO 2006/090392 A3

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/IL2006/000254

(22) International Filing Date:
26 February 2006 (26.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/655,442 24 February 2005 (24.02.2005) US

(71) Applicant *(for all designated States except US)*: **RSA SECURITY INC.** [US/US]; 174 Middlesex Turnpike, Bedford, Massachusetts 01730 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KLEIN, Amit** [IL/IL]; 31 A.d. Gordon St. (apt. 6), 46433 Herzliya (IL). **GOLAN, Zohar** [IL/IL]; Kibbutz Ein Hahoresh, 38980 Ein Hahoresh (IL).

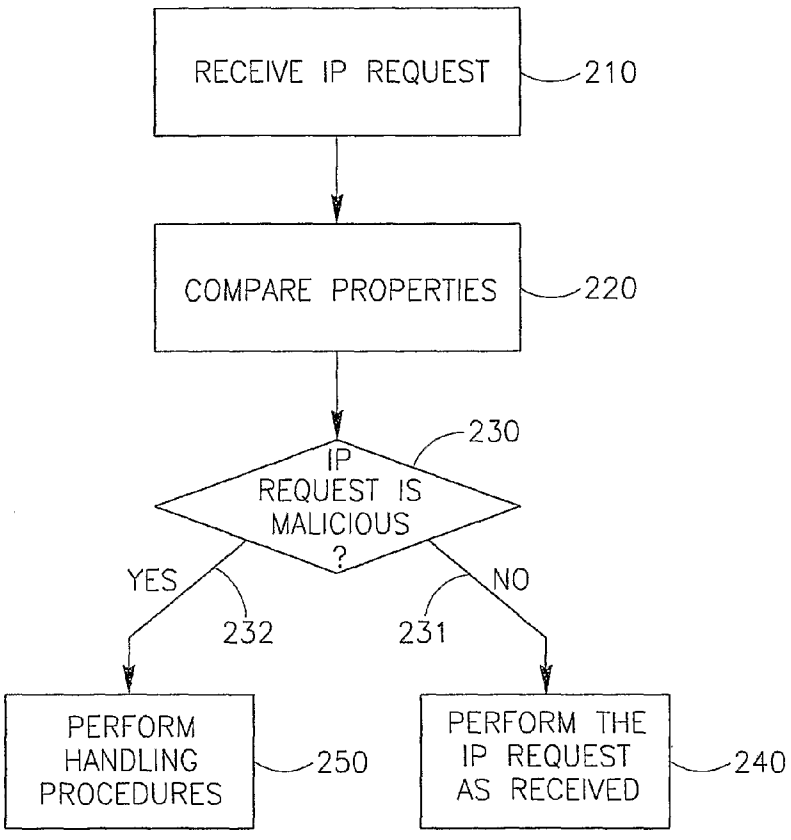
(74) Agent: **PEARL COHEN ZEDEK LATZER**; P.o. Box 12704, 46733 Herzelia (IL).

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR DETECTING AND MITIGATING DNS SPOOFING TROJANS



(57) Abstract: Embodiments of the present invention relate to a method and system for detecting and/or mitigating domain name system (DNS) spoofing Trojan horse (or Trojan) code. Trojan code (sometimes called malware or malicious software) is a common computer security problem. Some Trojans modify the DNS resolution mechanism employed by the infected computer, such that the computer traffic, when browsing the Internet, is routed to a location not intended by the rightful owner of the computer. The present invention can detect this phenomenon from a remote device or location and may take action to mitigate its effects.

WO 2006/090392 A3

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

(88) Date of publication of the international search report:
18 October 2007

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/IL06/00254

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06F 15/16**(2006.01)

USPC: 709/229
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. : 709/229

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 practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/0039827 A (THOMAS et al.) 26 February 2004 (26.02.2004) pages 1-17	1-52
A	US 2004/0103318 A (MILLER et al.) 27 May 2004 (27.05.2004)	1-52

☐ 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 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
23 June 2007 (23.06.2007)	01 AUG 2007
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 Larry D. Donaghue Jacqueline A. Whitfield Special Project Asst. Telephone No. 703-305-3900

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL06/00254

Continuation of B. FIELDS SEARCHED Item 3:
EAST, ACM
search terms: remote, redirect, server security