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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 October 2003 (30.10.2003)

PCT

(10) International Publication Number
WO 03/090426 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US03/11824

(22) International Filing Date: 15 April 2003 (15.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/373,135 17 April 2002 (17.04.2002) US

(71) Applicant: COMPUTER ASSOCIATES THINK, INC. [/US]; One Computer Associates Plaza, Islandia, NY 11749 (US).

(72) Inventor: KIDRON, Yaron; 100 North Whisman Road, #2314, Mountain View, CA 94043 (US).

(74) Agents: JAWORSKI, Richard, F. et al.; Cooper & Dunham LLP, 1185 Avenue of the Americas, New York, NY 10036 (US).

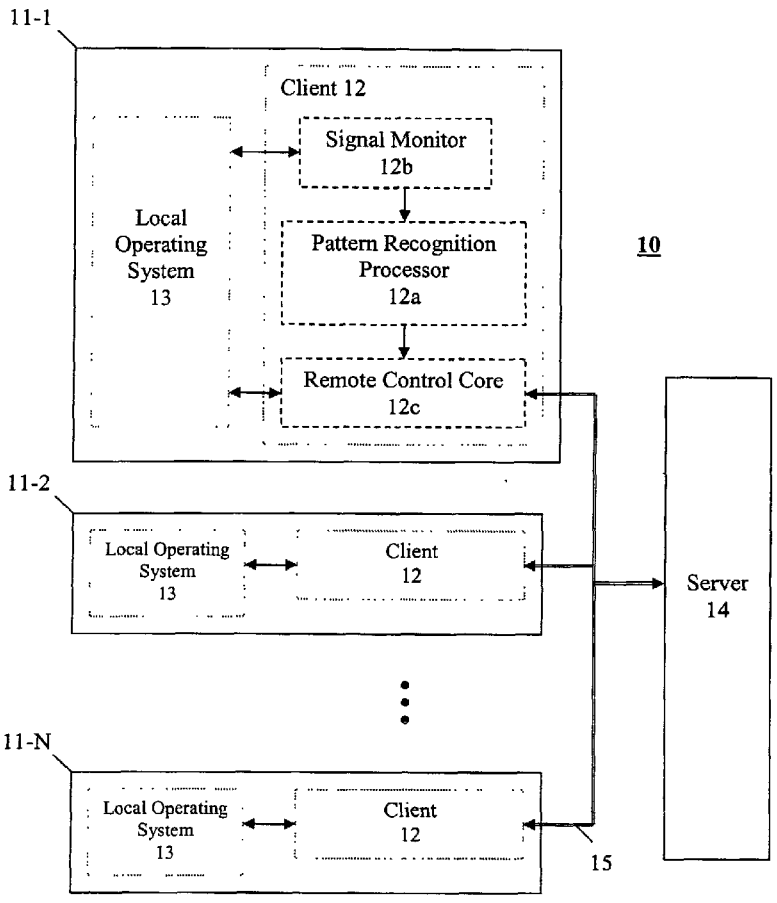
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (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 patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: DETECTING AND COUNTERING MALICIOUS CODE IN ENTERPRISE NETWORKS



(57) Abstract: A system and method for detecting and countering malicious code in an enterprise network are provided. A pattern recognition processor monitors local operations on a plurality of local machines connected through an enterprise network, to detect irregular local behavior patterns. An alert may be generated after an irregularity in behavior pattern on a local machine is detected. Irregular behavior alerts from a plurality of local machines are analyzed. If similar alerts are received from at least a threshold number of local machines over a corresponding period of time, one or more countermeasure operations are selected based on the analysis of the irregular behavior alerts. The selected countermeasure operations are communicated to the local machines and performed by the local machines.

WO 03/090426 A1

— *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.