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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 August 2015 (27.08.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/127472 A3

(51) **International Patent Classification:**
G06F 12/14 (2006.01) *G06F 11/00* (2006.01)

(21) **International Application Number:**
PCT/US2015/017389

(22) **International Filing Date:**
24 February 2015 (24.02.2015)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
61/944,006 24 February 2014 (24.02.2014) US
14/629,444 23 February 2015 (23.02.2015) US

(71) **Applicant: CYPHORT, INC.** [US/US]; 545 1 Great America Pkwy., Suite 225, Santa Clara, California 95054 (US).

(72) **Inventors: GOLSHAN, Ali;** 3595 Granada Avenue, Apt 416, Santa Clara, California 9505 1 (US). **GONG, Fengmin;** 2071 Hall Circle, Livermore, California 94550 (US). **JAS, Frank;** 28 Silver Birch Lane, Scotts Valley, California 95066 (US). **BILOGORSKIY, Nick;** 867 Lewis Avenue, Sunnyvale, California 94086 (US). **VU, Neal;** 4810 Tuscany Circle, San Jose, California 96135 (US). **LU, Chenghuai;** 34184 Duke Lane, Fremont, California 94555 (US). **BURT, Alex;** 7295 Via Vico, San Jose, California 95129 (US). **KENYAN, Manikandan;** 20644 Oak Creek Lane, Saratoga, California 95070 (US). **TING, Yucheng;** 1898 Shenandoah Avenue, Milpitas, California 95035 (US).

(74) **Agents: MOONEY, Christopher, M.** et al; 2 Palo Alto Square, Suite 500, 3000 El Camino Real, Palo Alto, California 94306-2106 (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, 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, KM, ML, MR, NE, SN, TD, TG).

[Continued on nextpage]

(54) **Title:** SYSTEMS AND METHODS FOR MALWARE DETECTION AND MITIGATION

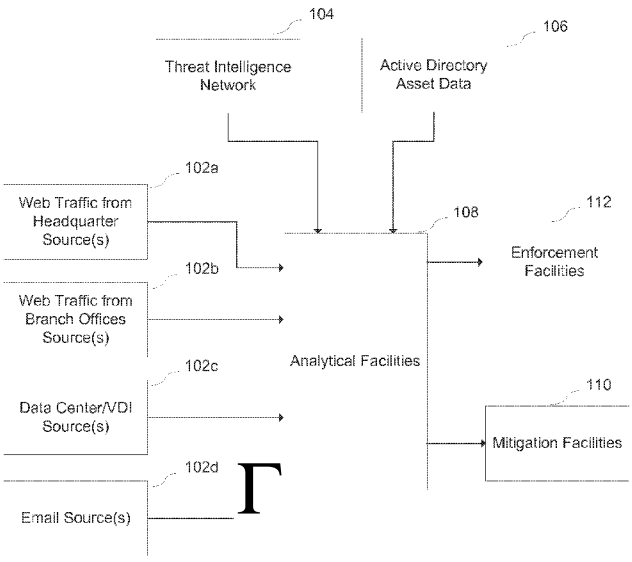

Figure 1

(57) **Abstract:** Systems and methods for monitoring malware events in a computer networking environment are described. The systems and methods including the steps of identifying a plurality of suspect objects comprising data about network transactions or computer operations suspected of being linked to a security risk; transmitting the suspect objects to an inspection service operating on one or more general purpose digital computers; transmitting said digital information to an analytical service operating on one or more general purpose digital computers; transmitting said one or more scores to a correlation facility which aggregates a plurality of scores, optionally with other information about each suspect objects, into the form of aggregate data representing one or more aggregate features of a plurality of suspect objects; and generating an infection verification pack comprising routines which, when run on an end-point machine within the computer networking environment, will mitigate a suspected security threat.

WO 2015/127472 A3

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:

4 February 2016

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 15/17389

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 12/14, G06F 11/00 (2015.01)
CPC - G06F 21/56
According to Internationa] Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
CPC: G06F21/56; IPC(8): G06F 12/14, G06F 11/00 (2015.01); USPC: 726/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC: H04L63/145, G06F21/56, G06F21/566, G06F21/564, G06F21/562; USPC: 726/22, 726/23, 726/24, 726/25, 726/26, 709/224
(keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Google Scholar
Search Terms: monitor, malware, network, suspect, security, risk, inspect, threat, score, mitigate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2013/0097706 A1 (TITONIS et al.) 18 April 2013 (18.04.2013), entire document, especially abstract and para [0013], [0015], [0023]-[0026], [0030], [0102], [01 10]-[0124], [0135], [0150]-[0151], [0210]-[021 1], [0223], [0228]-[0230], [0232]-[0233], [0262]-[0263], [0282]-[0309], [0317], [0344], [0353], [0395]-[0398], [0422]-[0424], [0427], [0432].	1, 3-7 ---------- 2
Y	US 2013/0318568 A1 (MAHAFFEY et al.) 28 November 2013 (28.1 1.2013), entire document, especially abstract and para [0078], [0091], [0095].	2
A	US 2013/0298244 A1 (KUMAR et al.) 07 November 2013 (07.1 1.2013), entire document.	1-7

☐ Further documents are listed in the continuation of Box C. ☐

* 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
20 October 2015 (20.10.2015)	11 DEC 2015

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)