



(51) International Patent Classification:

G06F 21/50 (2013.01) G06F 9/22 (2006.01)
G06F 15/16 (2006.01)

(21) International Application Number:

PCT/US2013/040420

(22) International Filing Date:

9 May 2013 (09.05.2013)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

13/492,672 8 June 2012 (08.06.2012) US

(71) Applicant: CROWDSTRIKE, INC. [US/US]; 30251 Golden Lantern, Laguna Niguel, CA 92677-5993 (US).

(72) Inventors: DIEHL, David, F.; 5324 Elliot Ave S, Minneapolis, MN 55417 (US). ALPERVOTICH, Dmitri; 7903 Plum Creek Drive, Gaithersburg, MD 20879 (US). IONESCU, Ion-Alexandru; 512 Van Ness, #302, San Francisco, CA 94102 (US). KURTZ, George, Robert;

27762 Antonio Pkway, L1-260, Ladera Ranch, CA 92694 (US).

(74) Agents: PECK, Robert, C. et al.; Lee & Hayes, PLLC, 601 W. Riverside Ave, Suite 1400, Spokane, WA 99201 (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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, SZ, TZ,

[Continued on next page]

(54) Title: KERNEL-LEVEL SECURITY AGENT

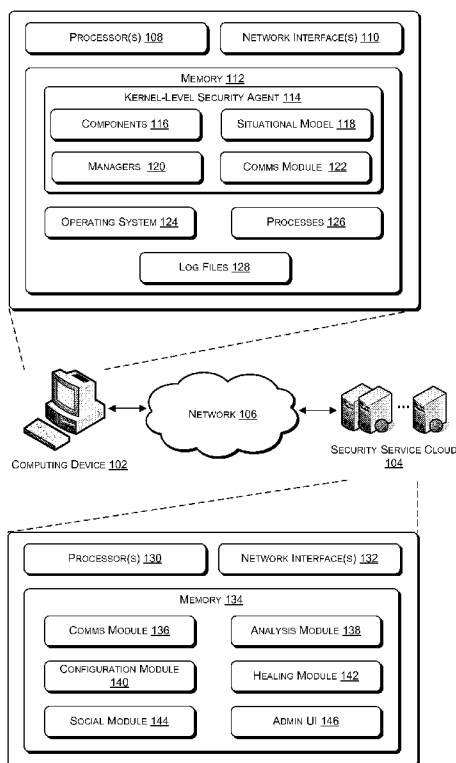


Fig. 1

(57) Abstract: A kernel-level security agent is described herein. The kernel-level security agent is configured to observe events, filter the observed events using configurable filters, route the filtered events to one or more event consumers, and utilize the one or more event consumers to take action based at least on one of the filtered events. In some implementations, the kernel-level security agent detects a first action associated with malicious code, gathers data about the malicious code, and in response to detecting subsequent action(s) of the malicious code, performs a preventative action. The kernel-level security agent may also deceive an adversary associated with malicious code. Further, the kernel-level security agent may utilize a model representing chains of execution activities and may take action based on those chains of execution activities.



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, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*