



- (51) **International Patent Classification:**
G06F 21/53 (2013.01) **G06F 9/455** (2006.01)
G06F 21/56 (2013.01)
- (21) **International Application Number:**
PCT/RO2014/000019
- (22) **International Filing Date:**
2 July 2014 (02.07.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/936,058 5 July 2013 (05.07.2013) US
- (71) **Applicant (for all designated States except US):** **BITDEFENDER IPR MANAGEMENT LTD** [—/CY]; Kreontos 12, PC 1076, Nicosia (CY).
- (72) **Inventors; and**
- (71) **Applicants (for US only):** **LUKACS, Sandor** [RO/RO]; Bld. Cetatea Fetei bl. 8, et. 3, Sat Florești (Com. Florești), Județ Cluj (RO). **TOȘA, Raul-Vasile** [RO/RO]; Str. Edgar Quinet nr. 32, et. 4, ap. 30, Cluj-Napoca, Județ Cluj (RO). **BOCA, Paul-Daniel** [RO/RO]; Str. Agricultorilor nr. 20, sc. 2, ap. 22, Cluj-Napoca, Județ Cluj (RO). **HAJMAȘAN, Gheorghe-Florin** [RO/RO]; Sat. Lunca Mureșului nr. 351, Comuna Lunca Mureșului, Județ Alba (RO). **LUȚAS, Andrei-Vlad** [RO/RO]; Bld. Cloșca nr.111, Satu Mare, Județ Satu Mare (RO).

(74) **Agent:** **TULUCA, Doina**; Bd. Lacul Tei 56, bl. 19, sc. B, ap. 52, sector 2, RO-020392 Bucuresti (RO).

(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, 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, 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, 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).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

[Continued on next page]

(54) **Title:** PROCESS EVALUATION FOR MALWARE DETECTION IN VIRTUAL MACHINES

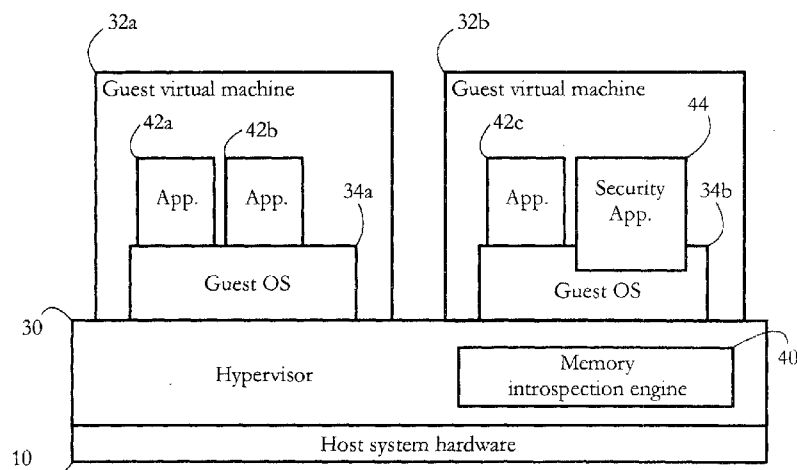


FIG. 2

(57) **Abstract:** Described systems and methods allow protecting a computer system from malware, such as viruses and rootkits. An anti-malware component executes within a virtual machine (VM) exposed by a hypervisor executing on the computer system. A memory introspection engine executes outside the virtual machine, at the processor privilege level of the hypervisor, and protects a process executing within the virtual machine by write-protecting a memory page of the respective process. By combining anti-malware components executing inside and outside the respective VM, some embodiments of the present invention may use the abundance of behavioral data that inside- VM components have access to, while protecting the integrity of such components from outside the respective VM.



-
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))* — *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))*
- Published:**
- *with international search report (Art. 21(3))*