

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
06 September 2024 (06.09.2024)



(10) International Publication Number
WO 2024/180211 A1

- (51) **International Patent Classification:**
G06F 21/55 (2013.01) *G06F 21/56* (2013.01)
- (21) **International Application Number:**
PCT/EP2024/055331
- (22) **International Filing Date:**
01 March 2024 (01.03.2024)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
18/177,396 02 March 2023 (02.03.2023) US
- (71) **Applicant: BITDEFENDER IPR MANAGEMENT LTD** [CY/CY]; 59-61 Acropolis ave. 3rd floor, office 302, Nicosia, 2012 (CY).
- (72) **Inventors: PORTASE, Radu-Marian**; Str. Anton Pann nr. 28-30, Corp B, sc. B, et. 4, ap. 47, Judetul Cluj, 400053 Cluj-Napoca (RO). **FULOP, Botond**; Str. Nădăsel nr. 68-74, bl.

B2, ap. 2, Judetul Cluj, 400207 Cluj-Napoca (RO). **HAJ-MASAN, Gheorghe Florin**; Str. Alexandru Vaida Voevod nr. 16, Corp IB, sc. 1, et. 6, ap. 37, Judetul Cluj, 400592 Cluj-Napoca (RO).

(74) **Agent: CABINET DOINA TULUCA**; Bd. Lacul Tei Nr. 56, bl. 19. sc. B, ap. 52, sector 2, 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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) **Title:** ANTIMALWARE SYSTEMS AND METHODS USING OPTIMAL TRIGGERING OF ARTIFICIAL INTELLIGENCE MODULES

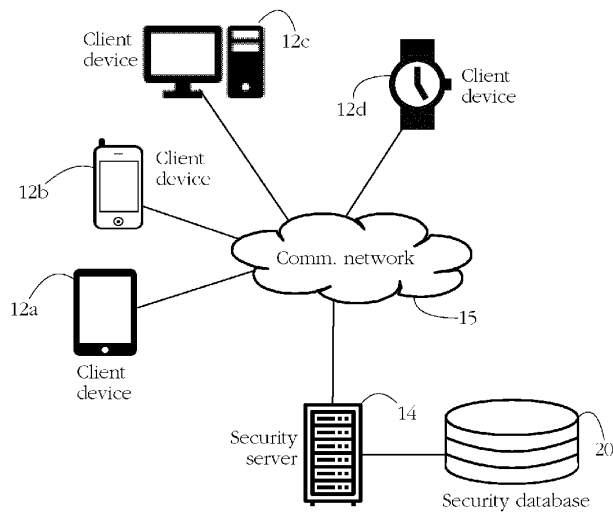


FIG. 1

(57) **Abstract:** Some embodiments determine optimal trigger events for executing a malware-detecting artificial intelligence (AI) module by tracking a performance of the respective module over a lifetime of each software sample of a training corpus. Computational costs associated with the respective AI module may be substantially reduced by executing the respective module only sporadically, in response to detecting an occurrence of one of the identified trigger events. In some embodiments, a malware detector employs multiple AI modules, each having its own specific triggers. The choice of triggers may be updated at any time, without affecting other aspects of the malware detector.

[Continued on next page]

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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).

Published:

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