



(51) International Patent Classification:
G06F 21/55 (2013.01)

(21) International Application Number:
PCT/EP2023/072883

(22) International Filing Date:
21 August 2023 (21.08.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17/821,493 23 August 2022 (23.08.2022) US

(71) Applicant: **BITDEFENDER IPR MANAGEMENT LTD** [CY/CY]; 58-61 Acropolis ave. 3rd floor, office 302, Nicosia, 2012 (CY).

(72) Inventors: **TIVADAR, Marius M.**; Ale. Serelor nr. 7 ap. 23 sc. C, Judet Maramures, 430233 Baia Mare (RO). **BO-CEREG, Alexandra S.**; Str. Victor Gaga nr. 10, Judet

Timis, 300695 Timisoara (RO). **GOSA, Razvan G.**; Loc. Lazaresti nr. 25, Judet Gorj, 215102 Bumbesti Jiu (RO).

(74) Agent: **TULUCA, Doina**; Bd. Lacul Tei nr. 56, bl. 19, 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.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV,

(54) Title: AGGREGATE EVENT PROFILES FOR DETECTING MALICIOUS MOBILE APPLICATIONS

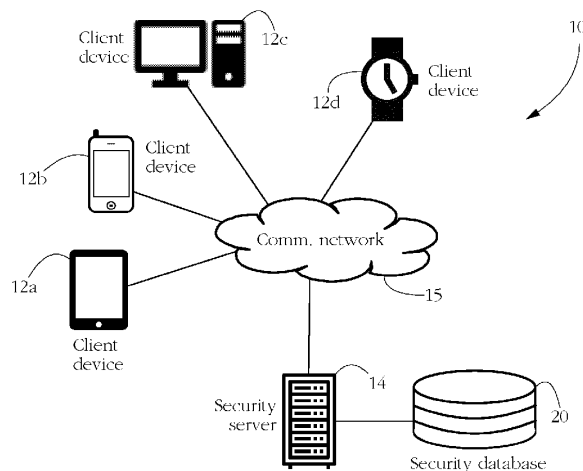


FIG. 1

(57) Abstract: Described systems and methods protect client devices such as personal computers and IoT devices against malicious software. In some embodiments, a plurality of client devices report the occurrence of various events to a security server, each such event caused by a local instance of a target application (e.g., mobile app) executing on a respective device. The security server then collates the behavior of the respective target application across the plurality of client devices. Some embodiments compute an aggregate event set and/or sequence combining events detected on one device with events detected on other devices, and determine whether the target application is malicious according to the aggregate event set/sequence.

[Continued on next page]

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))