

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
18 June 2020 (18.06.2020)



(10) International Publication Number
WO 2020/120428 A1

- (51) **International Patent Classification:**
G06F 21/55 (2013.01) *H04L 29/06* (2006.01)
- (21) **International Application Number:**
PCT/EP2019/084311
- (22) **International Filing Date:**
10 December 2019 (10.12.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
16/215,214 10 December 2018 (10.12.2018) US
- (71) **Applicant: BITDEFENDER IPR MANAGEMENT LTD** [CY/CY]; 59-61 Acropolis ave. 3rd floor, office 302, Nicosia, 2012 (CY).
- (72) **Inventors: DICHIU, Daniel**; Str. Piata Amzei, nr. 10-22, sc. D, ap. 73, Sector 1, 010345 Bucuresti (RO). **NICULAE, Stefan**; Str. Giurca Constantin nr. 9A, judet ILFOV, 077085 Dobroesti (RO). **BOSINCEANU, Elena A.**; Str. Liceului, nr. 2, judet Ialomita, 925100 Fetesti (RO). **ZAMFIR, Sorina N.**; Str. Ciresului, nr. 40A, et. 3, ap. A9, Sector 6, 024104 Bucuresti (RO). **DINCU, Andreea**; Str. Valea Calugareasca, nr. 4, bl. 5, sc. A, ap. 9, Sector 6, 061725 Bucuresti

(RO). **APOSTOAE, Andrei A.**; Sat Ciorani, judet Vrancea, 627276 Com. Pufesti (RO).

(74) **Agent: TULUCA, Doina**; Bd. Lacul Tei 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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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).

(54) **Title: SYSTEMS AND METHODS FOR BEHAVIORAL THREAT DETECTION**

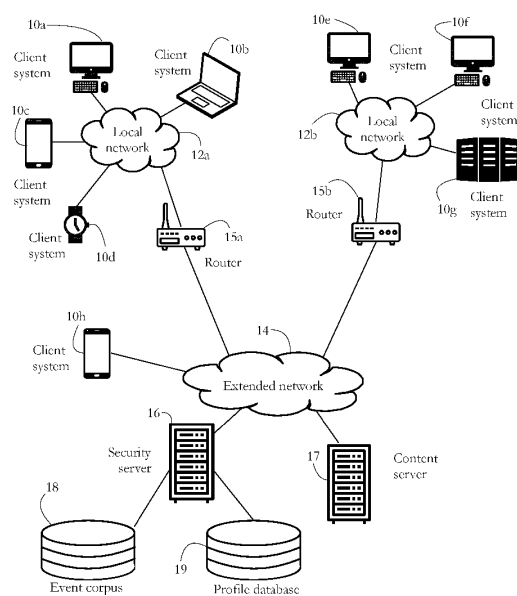


FIG. 1

(57) **Abstract:** In some embodiments, a behavioral computer security system protects clients and networks against threats such as malicious software and intrusion. A set of client profiles is constructed according to a training corpus of events occurring on clients, wherein each client profile represents a subset of protected machines, and each client profile is indicative of a normal or baseline pattern of using the machines assigned to the client respective profile. A client profile may group together machines having a similar event statistic. Following training, events detected on a client are selectively analyzed against a client profile associated with the respective client, to detect anomalous behavior. In some embodiments, individual events are analyzed in the context of other events, using a multi-dimensional event embedding space.

[Continued on next page]

Published:

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