



- (51) **International Patent Classification:**  
*G06F 21/56* (2013.01) *G06F 21/55* (2013.01)
- (21) **International Application Number:**  
PCT/EP2024/073956
- (22) **International Filing Date:**  
27 August 2024 (27.08.2024)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**  
18/461,134 05 September 2023 (05.09.2023) US  
18/461,251 05 September 2023 (05.09.2023) 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, 40053

Cluj-Napoca (RO). **HASMASAN, Gheorghe Florin**; Str. Alexandru Vaida Voevod nr. 16, Corp 1B, sc. 1, et. 6, ap. 37, Judetul Cluj, 400592 Cluj-Napoca (RO). **HAJMASAN, Alexandra**; Str. Alexandru Vaida Voevod, nr. 16, Corp 18, sc. 1, et. 6, ap. 37, Judetul Cluj, 400592 Cluj-Napoca (RO).

(74) **Agent: TULUCA, DOINA / 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,

(54) **Title: SYSTEMS AND METHODS FOR COUNTERING PERSISTENT MALWARE**

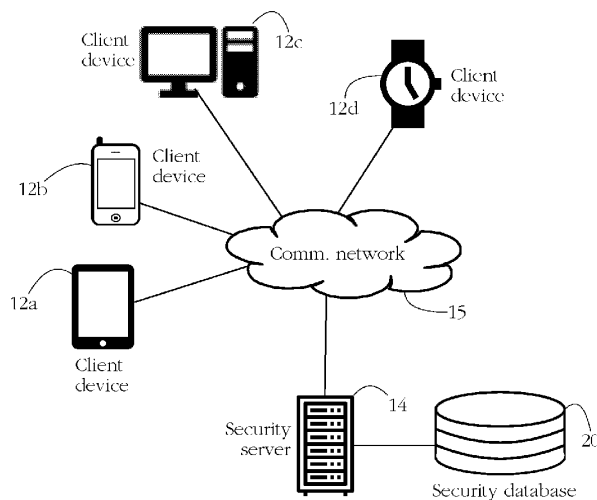


FIG. 1

(57) **Abstract:** Some embodiments construct an entity map describing a group of inter-related entities and determine whether a computing device comprises malware according to the respective entity map. The entity map includes worker entities (e.g., processes) and resource entities (e.g., files) accessed by the respective worker entities. Some entity maps are persistently stored and recovered in response to a reboot, enabling a complete reconstruction of a kill chain even when malicious activities are distributed among multiple entities and multiple computing sessions. Some embodiments detect infection by comparing a current entity map with a signature map describing at least a fragment of a known attack.

[Continued on next page]

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, 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))