

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
03 October 2019 (03.10.2019)



(10) International Publication Number
WO 2019/186535 A1

- (51) **International Patent Classification:**
H04L 29/06 (2006.01) *G06F 21/55* (2013.01)
- (21) **International Application Number:**
PCT/IL2019/050331
- (22) **International Filing Date:**
25 March 2019 (25.03.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
258345 25 March 2018 (25.03.2018) IL
- (71) **Applicants:** **B. G. NEGEV TECHNOLOGIES & APPLICATIONS LTD., AT BEN-GURION** [IL/IL]; 77 HaEnergia Street, POB 653, 8410501 Beer-Sheva (IL). **NANYANG TECHNOLOGICAL UNIVERSITY** [SG/SG]; N4-B2B-05, Nanyang Avenue, Singapore 639798 (SG).
- (72) **Inventors:** **ELOVICI, Yuval**; 9 Moshav Arugot, 7986400 D.N. Lachish (IL). **PUZIS, Rami**; 7 Hamelech Yerovam Street, 7748707 Ashdod (IL). **ZILBERMAN, Polina**; 58 Eshkolot, 8537700 Eshkolot (IL). **MARCO, Elad**; 13 Derech Mezada, 8435712 Beer Sheva (IL). **ELITZUR, Aviad**; 3 Mishol Ha'Arava, Sderot (IL). **SRIKANTHAN,**

Thambipillai; School of Computer Science & Engineering, N4-B2B-05, Nanyang Avenue, Singapore 639798 (SG). **CHATTOPADHYAY, Anupam**; School of Computer Science & Engineering, N4-B2B-05, Nanyang Avenue, Singapore 639798 (SG). **SIEW KEI, Lam**; School of Computer Science & Engineering, N4-B2B-05, Nanyang Avenue, Singapore 639798 (SG). **HAJ YAHYA, Jawad**; School of Computer Science & Engineering, N4-B2B-05, Nanyang Avenue, Singapore 639798 (SG).

(74) **Agent:** **LUZZATO, Kfir** et al.; Luzzatto & Luzzatto, P.O. Box 5352, 8415202 Beer Sheva (IL).

(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,

(54) **Title:** BIO-INSPIRED AGILE CYBER-SECURITY ASSURANCE FRAMEWORK

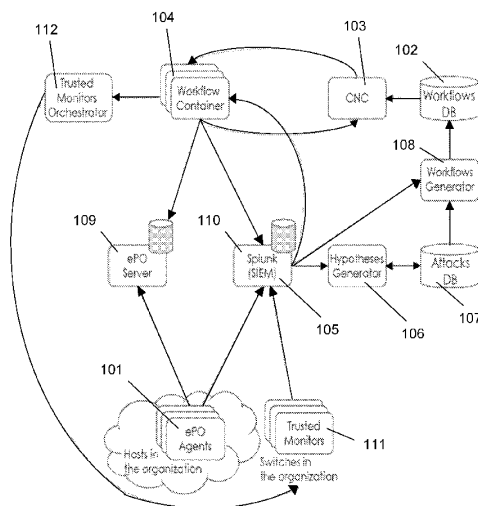


Fig. 1

(57) **Abstract:** A framework for efficiently and automatically exploring a data network and accurately identifying network threats, which comprises a plurality of software and hardware-based agents, distributed over the data network. The agents are capable of adjusting or reconfiguring, on the fly, the behavior of the agents and their ability to collect data in a targeted manner, so as to investigate suspicious incidents and alerts and collect data that was not yet collected by the system; collecting forensic data by executing tasks defined in workflows, being distributed threat intercepting programs and reporting about the collected forensic data, back to a Central Control Unit (C&C). Distributed threat intercepting programs ("workflows") are used to provide instructions to agents, to perform branching and provide instructions to the Central Control Unit (C&C), which orchestrates the agents to assure proper execution of the workflows; analyzes the collected information and presents ongoing status to an operator supervising the data network.

[Continued on next page]

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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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