

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
10 September 2021 (10.09.2021)



(10) International Publication Number
WO 2021/177989 A1

- (51) **International Patent Classification:**
G06F 12/14 (2006.01) *G06F 11/00* (2006.01)
- (21) **International Application Number:**
PCT/US2020/034280
- (22) **International Filing Date:**
22 May 2020 (22.05.2020)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/984,140 02 March 2020 (02.03.2020) US
- (71) **Applicant:** INTEL 471 INC. [US/US]; 16192 Coastal Highway, Lewes, DE 19958 (US).
- (72) **Inventors:** SUMMERLIN, Nick; 16192 Coastal Highway, Lewes, DE 19958 (US). PICHEL, Ferran; 16192 Coastal Highway, Lewes, DE 19958 (US).
- (74) **Agent:** WOJTALEWICZ, Kathy; PCK IP Lawyers (USA) P.C., 1717 Pennsylvania Avenue North West, Suite 1025, Washington, DC 20006 (US).
- (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, 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, 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).

Published:

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

- (54) **Title:** AUTOMATED MALWARE MONITORING AND DATA EXTRACTION

(57) **Abstract:** A malware monitoring method includes: obtaining a malware sample; extracting operational parameters corresponding to the malware sample; configuring an emulator application corresponding to the malware sample using the operational parameters; executing a plurality of instances of the configured emulator application; collecting output data from each of the plurality of instances; and generating indicators of compromise (IOCs) based on the collected output data.

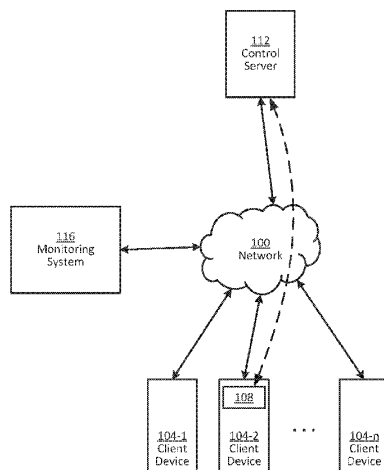


FIG. 1

WO 2021/177989 A1