



(51) International Patent Classification:
G06F 21/56 (2013.01)

(21) International Application Number:
PCT/US2014/040748

(22) International Filing Date:
3 June 2014 (03.06.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/953,608 29 July 2013 (29.07.2013) US

(71) Applicant: CROWDSTRIKE, INC. [US/US]; 15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618 (US).

(72) Inventor: GEFNER, Jason; 360 Nueces St. #1616, Austin, TX 78701 (US).

(74) Agents: ROHWER, Jacob P. et al.; Lee & Hayes, PLLC, 601 W. Riverside Ave, Suite 1400, Spokane, WA 99201 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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).

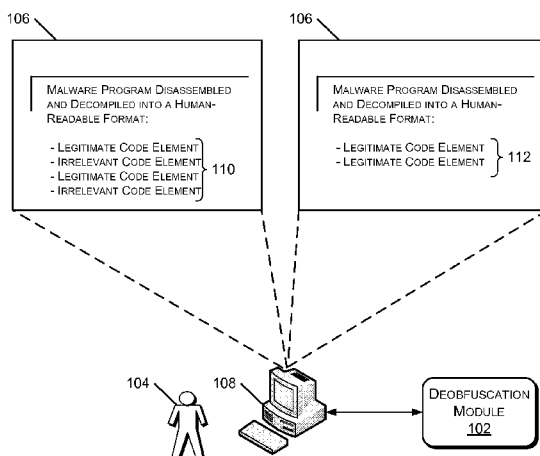
Published:

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

(54) Title: IRRELEVANT CODE IDENTIFICATION

100

FIG. 1



(57) Abstract: The techniques described herein identify, and/or distinguish between, legitimate code and/or irrelevant code in programs so that an analyst does not have to spend additional time sifting through and/or considering the irrelevant code when viewing the code of the program. Therefore, the analyst can be more efficient when determining a type of a program (e.g., malware) and/or when determining the actions of the program. For instance, a security researcher may be tasked with identifying the malware and/or determining the harmful or deceptive actions the malware executes on a computer (e.g., deletion of a file, the targeting of sensitive information such as social security numbers or credit card numbers, etc.).