



(51) International Patent Classification:

H04L 29/06 (2006.01) H04W 12/02 (2009.01)
H04W 12/00 (2009.01) H04L 12/58 (2006.01)

(21) International Application Number:

PCT/EP2020/068644

(22) International Filing Date:

02 July 2020 (02.07.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/405,140 07 May 2019 (07.05.2019) US

(71) Applicant: **BITDEFENDER IPR MANAGEMENT LTD** [CY/CY]; 59-61 Acropolis ave. 3rd floor, office 302, Nicosia, 2012 (CY).

(72) Inventor: **MIRCESCU, Daniel-Alexandru**; Str. Cozla nr. 8 bl.A7 sc.2 et.1 ap. 20, Sector 3, 032734 BUCURESTI (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, IT, 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).

(54) Title: SYSTEMS AND METHODS FOR USING DNS MESSAGES TO SELECTIVELY COLLECT COMPUTER FORENSIC DATA

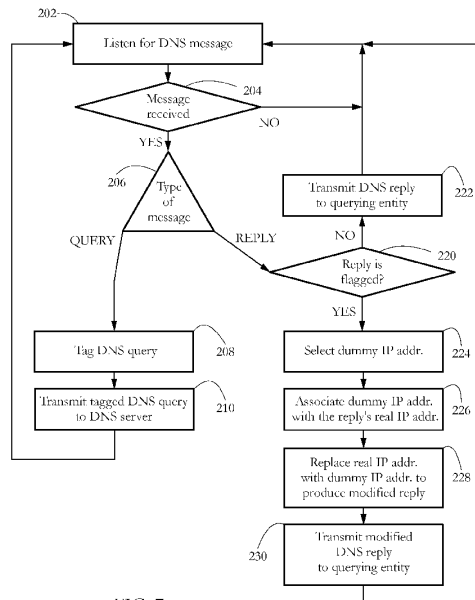


FIG. 7

(57) Abstract: Described systems and methods allow a selective collection of computer security data from client devices such as personal computers, smartphones, and Internet of Things (IoT) devices. A security application executing on each client device comprises a domain name service (DNS) proxy that tags outgoing DNS messages with a client ID. The DNS server selects a client for data collection by returning a DNS reply comprising a service activation flag. Some embodiments thus enable a per-DNS-message selectivity of data collection. In some embodiments, subsequent network access requests by the selected clients are re-routed to a security server for analysis.

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *with information concerning request for restoration of the right of priority in respect of one or more priority claims (Rules 26bis.3 and 48.2(b)(vii))*