



(43) International Publication Date
12 September 2014 (12.09.2014)

- (51) International Patent Classification:
G06F 21/55 (2013.01) *G06F 11/30* (2006.01)
- (21) International Application Number:
PCT/US2014/017950
- (22) International Filing Date:
24 February 2014 (24.02.2014)
- (25) Filing Language:
English
- (26) Publication Language:
English
- (30) Priority Data:
13/784,720 4 March 2013 (04.03.2013) US
- (71) Applicant: **CROWDSTRIKE, INC.** [US/US]; 30251 Golden Lantern, Suite E-519, Laguna Niguel, CA 92677-5993 (US).
- (72) Inventors: **MEYERS, Adam, S.**; 630 C Street SE, Washington, DC 20003 (US). **ALPEROVITCH, Dmitri**; 7903 Plum Creek Drive, Gaithersburg, MD 20879 (US). **KURTZ, George, Robert**; 27762 Antonio Pkway, L1-260, Ladera Ranch, CA 92694 (US). **DIEHL, David, F.**; 5324

Elliot Ave S, Minneapolis, MN 55417 (US). **KRASSER, Sven**; 135 W Del Mar Blvd, Apt 1108, Pasadena, CA 91105 (US).

(74) Agents: **PECK, Robert, C.** 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,

[Continued on next page]

(54) Title: DECEPTION-BASED RESPONSES TO SECURITY ATTACKS

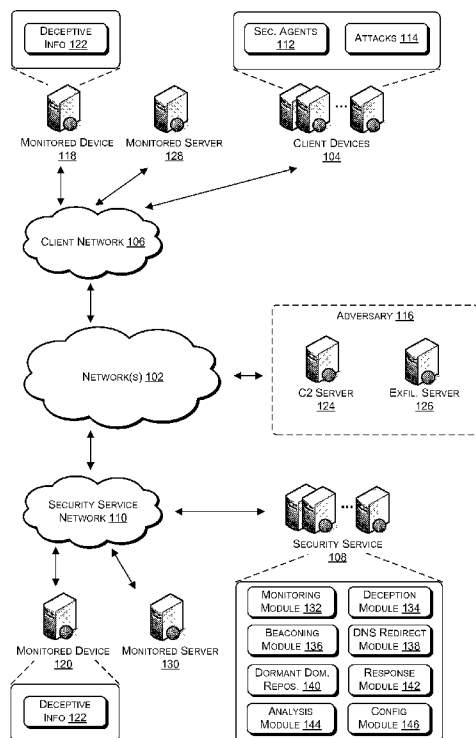


Fig. 1

(57) Abstract: Deception-based techniques for responding to security attacks are described herein. The techniques include transitioning a security attack to a monitored computing device posing as a computing device impacted by the security attack and enabling the adversary to obtain deceptive information from the monitored computing device. Also, the adversary may obtain a document configured to report identifying information of an entity opening the document, thereby identifying the adversary associated with the attack. Further, the techniques include determining that a domain specified in a domain name request is associated with malicious activity and responding to the request with a network address of a monitored computing device to cause the requesting process to communicate with the monitored computing device in place of an adversary server. Additionally, a service may monitor dormant domains names associated with malicious activity and, in response to a change, respond with an alert or a configuration update.



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))