

CORRECTED VERSION

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
23 October 2014 (23.10.2014)



(10) International Publication Number
WO 2014/172182 A8

(51) International Patent Classification:
G06F 21/50 (2013.01)

(21) International Application Number:
PCT/US2014/033661

(22) International Filing Date:
10 April 2014 (10.04.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/866,968 19 April 2013 (19.04.2013) US

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

(72) Inventor: **IONESCU, Ion-Alexandru**; 512 Van Ness, #302, San Francisco, CA 94102 (CA).

(74) Agents: **LEE, Lewis, 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, 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))

(48) Date of publication of this corrected version:

4 June 2015

(15) Information about Correction:
see Notice of 4 June 2015

(54) Title: EXECUTABLE COMPONENT INJECTION UTILIZING HOTPATCH MECHANISMS

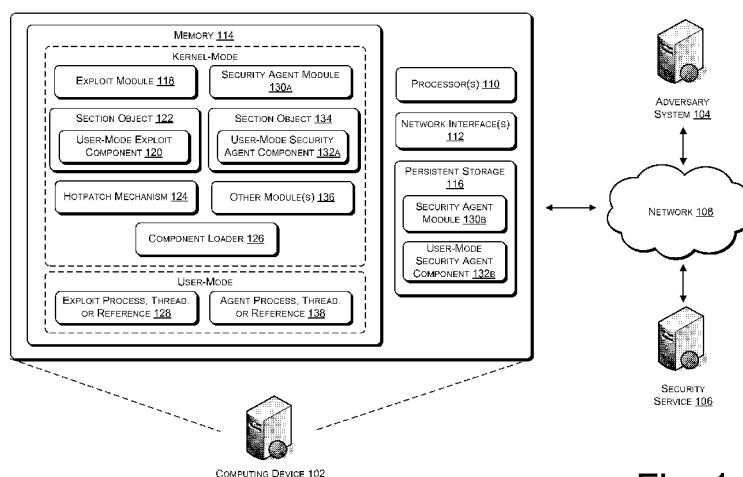


Fig. 1

(57) Abstract: Techniques for causing a component loader associated with a hotpatch mechanism to execute a user-mode component which, when executed, creates a user-mode process, thread, or held reference are described herein. The component may further indicate to the component loader that it lacks hotpatch data, causing the component loader to unload the component. In some implementations, a kernel-mode module may initially provide the component to the hotpatch mechanism with an entrypoint of the component set to zero and with hotpatch data for the component loader. The hotpatch mechanism may apply the hotpatch data, modifying the component loader such that the component loader requests execute rights for a section object for the component. The kernel-mode module may then set the entrypoint such that the component becomes executable, and provides the section object and component to the hotpatch mechanism to cause the component loader to execute the component.